SOIP0811 US00

日 本 国 特 許 庁
JAPAN PATENT OFFICE

#5

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年 ４月 ２日

出願番号
Application Number: 特願２００１－１０３１５３

出願人
Applicant(s): ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年 ５月１１日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

【書類名】　特許願
【整理番号】　0100242111
【提出日】　平成13年 4月 2日
【あて先】　特許庁長官殿
【国際特許分類】　H04N 7/08
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　江▲崎▼　正
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　平井　純
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　佐藤　英雄
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
　【代表者】　出井　伸之
【代理人】
　【識別番号】　100101801
　【弁理士】
　【氏名又は名称】　山田　英治
【選任した代理人】
　【識別番号】　100093241
　【弁理士】
　【氏名又は名称】　宮田　正昭

【選任した代理人】

【識別番号】　100086531

【弁理士】

【氏名又は名称】　澤田　俊夫

【先の出願に基づく優先権主張】

【出願番号】　特願2000-162319

【出願日】　平成12年 5月31日

【手数料の表示】

【予納台帳番号】　062721

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9904833

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　コンテンツ・コピー管理システム及び方法、情報処理装置及び方法、サーバ、並びに、記憶媒体

【特許請求の範囲】

【請求項１】

コンテンツの外部機器へのコピーを管理するコンテンツ・コピー管理システムであって、

コピー対象となるコンテンツを読み込む手段と、

コピー対象となるコンテンツの識別情報を読み込む手段と、

各コンテンツのコピー可否情報を保管するデータベースと、

コンテンツに挿入された電子透かしを検査する電子透かし検査手段と、

コンテンツの外部機器へのコピー動作を制御するコピー制御手段と、

を具備し、

前記コピー制御手段は、コピー対象となるコンテンツの識別情報及び／又は属性情報を基に前記データベースを検索し、該当するレコードが存在する場合にはそのレコードの内容に応じてコピー動作を制御し、該当するレコードが存在しない場合には前記電子透かし検査手段による該コンテンツの検査結果に応じてコピー動作を制御することを特徴とするコンテンツ・コピー管理システム。

【請求項２】

前記コピー制御手段は、コンテンツを圧縮及び暗号化してから前記外部機器にコピーすることを特徴とする請求項１に記載のコンテンツ・コピー管理システム。

【請求項３】

前記コピー制御手段と前記データベースは安全な通信路を介して接続されていることを特徴とする請求項１に記載のコンテンツ・コピー管理システム。

【請求項４】

さらに、コピー対象となるコンテンツの属性情報を取得する手段を備え、

前記属性情報は、コンテンツの一部を切り取ったデータであることを特徴とする請求項１に記載のコンテンツ・コピー管理システム。

【請求項５】

さらに、コピー対象となるコンテンツの属性情報を取得する手段を備え、

前記属性情報は、コンテンツの一部又は全部のハッシュ値であることを特徴とする請求項１に記載のコンテンツ・コピー管理システム。

【請求項６】

さらに、コピー対象となるコンテンツの属性情報を取得する手段を備え、

前記属性情報は、コンテンツのエンベロープ値、リズムに相当する周期、スペクトルの広がり方などのコンテンツに関する特徴値又は特徴量であることを特徴とする請求項１に記載のコンテンツ・コピー管理システム。

【請求項７】

コンテンツの外部機器へのコピーを管理するコンテンツ・コピー管理方法であって、

コピー対象となるコンテンツを読み込むステップと、

コピー対象となるコンテンツの識別情報を読み込むステップと、

コピー対象となるコンテンツの識別情報及び／又は属性情報を基にして各コンテンツのコピー可否情報を保管するデータベースに対して問い合わせるステップと、

該データベース中に該当するレコードが存在する場合にはそのレコードの内容に応じてコピー動作を制御するステップと、

該データベース中に該当するレコードが存在しない場合にはコンテンツ中に挿入された電子透かしの検査結果に応じてコピー動作を制御するステップと、

を具備することを特徴とするコンテンツ・コピー管理方法。

【請求項８】

前記コピー動作を制御するステップでは、コンテンツを圧縮及び暗号化してから前記外部機器にコピーすることを特徴とする請求項７に記載のコンテンツ・コピー管理方法。

【請求項９】

前記データベースへの問合せは安全な通信路を介して行われることを特徴とする請求項７に記載のコンテンツ・コピー管理方法。

【請求項１０】

さらに、コピー対象となるコンテンツの属性情報を取得するステップを備え、

前記属性情報は、コンテンツの一部又は全部を切り取ったデータであることを特徴とする請求項７に記載のコンテンツ・コピー管理方法。

【請求項１１】

さらに、コピー対象となるコンテンツの属性情報を取得するステップを備え、

前記属性情報は、コンテンツの一部又は全部のハッシュ値であることを特徴とする請求項７に記載のコンテンツ・コピー管理方法。

【請求項１２】

さらに、コピー対象となるコンテンツの属性情報を取得するステップを備え、

前記属性情報は、コンテンツのエンベロープ値、リズムに相当する周期、スペクトルの広がり方などのコンテンツに関する特徴値又は特徴量であることを特徴とする請求項７に記載のコンテンツ・コピー管理方法。

【請求項１３】

コンテンツの外部機器へのコピー動作を実行する情報処理装置であって、

コピー対象となるコンテンツを読み込む手段と、

コピー対象となるコンテンツの識別情報を読み込む手段と、

コンテンツに挿入された電子透かしを検査する電子透かし検査手段と、

コンテンツの外部機器へのコピー動作を制御するコピー制御手段と、

を具備し、

前記コピー制御手段は、コピー対象となるコンテンツの識別情報及び／又は属性情報を基に外部サーバに対して問合せを行い、該問合せ結果に応じて、コンテンツのコピー動作を実行するか、又は、前記電子透かし検査手段による該コンテンツの検査を実行して該検査結果に従ってコピー動作を制御することを特徴とする情報処理装置。

【請求項１４】

前記コピー制御手段は、コンテンツを圧縮及び暗号化してから前記外部機器にコピーすることを特徴とする請求項１３に記載の情報処理装置。

【請求項１５】

前記外部サーバとは安全な通信路を介して接続されていることを特徴とする請求項１３に記載の情報処理装置。

【請求項１６】

さらに、コピー対象となるコンテンツの属性情報を取得する手段を備え、

前記属性情報は、コンテンツの一部を切り取ったデータであることを特徴とする請求項１３に記載の情報処理装置。

【請求項１７】

さらに、コピー対象となるコンテンツの属性情報を取得する手段を備え、

前記属性情報は、コンテンツの一部又は全部のハッシュ値であることを特徴とする請求項１３に記載の情報処理装置。

【請求項１８】

さらに、コピー対象となるコンテンツの属性情報を取得する手段を備え、

前記属性情報は、コンテンツのエンベロープ値、リズムに相当する周期、スペクトルの広がり方などのコンテンツに関する特徴値又は特徴量であることを特徴とする請求項１３に記載の情報処理装置。

【請求項１９】

コンテンツの外部機器へのコピー動作を実行する情報処理方法であって、

コピー対象となるコンテンツを読み込むステップと、

コピー対象となるコンテンツの識別情報を読み込むステップと、

コピー対象となるコンテンツの識別情報及び／又は属性情報を基に外部サーバに対して問合せを行うステップと、

該問合せ結果に応じて、コンテンツのコピー動作を実行するか、又は、コンテンツに挿入された電子透かしの検査を実行して該検査結果に従ってコピー動作を制御するステップと、

を具備することを特徴とする情報処理方法。

【請求項２０】

前記コピー動作を制御するステップでは、コンテンツを圧縮及び暗号化してから前記外部機器にコピーすることを特徴とする請求項１９に記載の情報処理方法。

【請求項２１】

前記外部サーバへの問合せは安全な通信路を介して行うことを特徴とする請求項１９に記載の情報処理方法。

【請求項２２】

さらに、コピー対象となるコンテンツの属性情報を取得するステップを備え、

前記属性情報は、コンテンツの一部を切り取ったデータであることを特徴とする請求項１９に記載の情報処理方法。

【請求項２３】

さらに、コピー対象となるコンテンツの属性情報を取得するステップを備え、

前記属性情報は、コンテンツの一部又は全部のハッシュ値であることを特徴とする請求項１９に記載の情報処理方法。

【請求項２４】

さらに、コピー対象となるコンテンツの属性情報を取得するステップを備え、

前記属性情報は、コンテンツのエンベロープ値、リズムに相当する周期、スペクトルの広がり方などのコンテンツに関する特徴値又は特徴量であることを特徴とする請求項１９に記載の情報処理方法。

【請求項２５】

各コンテンツに関するコピー可否情報を管理するサーバであって、

コンテンツの識別情報及び／又は属性情報を基に検索可能なデータベースと、

コンテンツのコピー可否に関する問合せを受信する受信手段と、

該問合せに応答して前記データベースを検索する検索手段と、

前記データベースの検索結果を問い合わせ元に送信する送信手段と、

を具備することを特徴とするサーバ。

【請求項２６】

問合せ元とは安全な通信路を介して接続されることを特徴とする請求項２５に記載のサーバ。

【請求項２７】

前記属性情報は、コンテンツの一部を切り取ったデータであることを特徴とする請求項２５に記載のサーバ。

【請求項２８】

前記属性情報は、コンテンツの一部又は全部のハッシュ値であることを特徴とする請求項２５に記載のサーバ。

【請求項２９】

前記属性情報は、コンテンツのエンベロープ値、リズムに相当する周期、スペクトルの広がり方などのコンテンツに関する特徴値又は特徴量であることを特徴とする請求項２５に記載のサーバ。

【請求項３０】

コンテンツの外部機器へのコピーを管理する処理をコンピュータ・システム上で実行するためのコンピュータ・ソフトウェアをコンピュータ可読形式で物理的に格納したソフトウェア記憶媒体であって、前記コンピュータ・ソフトウェアは、

コピー対象となるコンテンツを読み込むステップと、

コピー対象となるコンテンツの識別情報を読み込むステップと、

コピー対象となるコンテンツの属性情報を取得するステップと、

コピー対象となるコンテンツの識別情報及び／又は属性情報を基にして各コンテンツのコピー可否情報を保管するデータベースに対して問い合わせるステップと、

該データベース中に該当するレコードが存在する場合にはそのレコードの内容に応じてコピー動作を制御するステップと、

該データベース中に該当するレコードが存在しない場合にはコンテンツ中に挿入された電子透かしの検査結果に応じてコピー動作を制御するステップと、

を具備することを特徴とするソフトウェア記憶媒体。

【請求項３１】

前記属性情報は、コンテンツの一部又は全部を切り取ったデータであることを特徴とする請求項３０に記載のソフトウェア記憶媒体。

【請求項３２】

前記属性情報は、コンテンツの一部又は全部のハッシュ値であることを特徴とする請求項３０に記載のソフトウェア記憶媒体。

【請求項３３】

前記属性情報は、コンテンツのエンベロープ値、リズムに相当する周期、スペクトルの広がり方などのコンテンツに関する特徴値又は特徴量であることを特徴とする請求項３０に記載のソフトウェア記憶媒体。

【請求項３４】

コンテンツの外部機器へのコピーを実行する処理をコンピュータ・システム上で実行するためのコンピュータ・ソフトウェアをコンピュータ可読形式で物理的に格納したソフトウェア記憶媒体であって、前記コンピュータ・ソフトウェアは、

コピー対象となるコンテンツを読み込むステップと、

コピー対象となるコンテンツの識別情報を読み込むステップと、

コピー対象となるコンテンツの属性情報を取得するステップと、

コピー対象となるコンテンツの識別情報及び／又は属性情報を基に外部サーバに対して問合せを行うステップと、

該問合せ結果に応じて、コンテンツのコピー動作を実行するか、又は、コンテンツに挿入された電子透かしの検査を実行して該検査結果に従ってコピー動作を制御するステップと、

を具備することを特徴とするソフトウェア記憶媒体。

【請求項３５】

前記属性情報は、コンテンツの一部又は全部を切り取ったデータであることを特徴とする請求項３４に記載のソフトウェア記憶媒体。

【請求項３６】

前記属性情報は、コンテンツの一部又は全部のハッシュ値であることを特徴とする請求項３４に記載のソフトウェア記憶媒体。

【請求項３７】

前記属性情報は、コンテンツのエンベロープ値、リズムに相当する周期、スペクトルの広がり方などのコンテンツに関する特徴値又は特徴量であることを特徴とする請求項３４に記載のソフトウェア記憶媒体。

【請求項３８】

コンテンツの外部機器へのコピーを管理するコンテンツ・コピー管理システムであって、

コピー対象となるコンテンツを読み込む手段と、

コピー対象となるコンテンツの識別情報を読み込む手段と、

各コンテンツのコピー可否情報を保管するデータベースと、

コンテンツに挿入された電子透かしを検査する電子透かし検査手段と、

コンテンツを直交変換する直交変換手段と、

直交変換後のコンテンツを量子化及びハフマン符号化する符号化圧縮手段と、

前記符号化圧縮されたコンテンツを暗号化する暗号化手段と、

コンテンツの外部機器への該暗号化コンテンツのコピー動作を制御するコピー制御手段と、

を具備し、

前記コピー制御手段は、コピー対象となるコンテンツの識別情報とコンテンツの直交変換値又はそのハッシュ値を基に前記データベースを検索し、該当するレコードが存在する場合にはそのレコードの内容に応じて該暗号化コンテンツのコピー動作を制御し、該当するレコードが存在しない場合には前記電子透かし検査手段による該コンテンツの検査結果に応じて該暗号化コンテンツのコピー動作を制御することを特徴とするコンテンツ・コピー管理システム。

【請求項３９】

コンテンツの外部機器へのコピーを管理するコンテンツ・コピー管理方法であって、

コピー対象となるコンテンツを読み込むステップと、

コピー対象となるコンテンツの識別情報を読み込むステップと、

コンテンツを直交変換する直交変換ステップと、

直交変換後のコンテンツを量子化及びハフマン符号化する符号化圧縮ステップと、

前記符号化圧縮されたコンテンツを暗号化する暗号化ステップと、

コピー対象となるコンテンツの識別情報とコンテンツの直交変換値又はそのハッシュ値を基にして各コンテンツのコピー可否情報を保管するデータベースに対

して問い合わせるステップと、

該データベース中に該当するレコードが存在する場合にはそのレコードの内容に応じて該暗号化コンテンツのコピー動作を制御するステップと、

該データベース中に該当するレコードが存在しない場合にはコンテンツ中に挿入された電子透かしの検査結果に応じて該暗号化コンテンツのコピー動作を制御するステップと、

を具備することを特徴とするコンテンツ・コピー管理方法。

【請求項４０】

コンテンツの外部機器へのコピー動作を実行する情報処理装置であって、

コピー対象となるコンテンツを読み込む手段と、

コピー対象となるコンテンツの識別情報を読み込む手段と、

コンテンツに挿入された電子透かしを検査する電子透かし検査手段と、

コンテンツを直交変換する直交変換手段と、

直交変換後のコンテンツを量子化及びハフマン符号化する符号化圧縮手段と、

前記符号化圧縮されたコンテンツを暗号化する暗号化手段と、

コンテンツの外部機器への該暗号化コンテンツのコピー動作を制御するコピー制御手段と、

を具備し、

前記コピー制御手段は、コピー対象となるコンテンツの識別情報とコンテンツの直交変換値又はそのハッシュ値を基に外部サーバに問合せを行い、該問合せ結果に応じて、該暗号化コンテンツのコピー動作を実行するか、又は、前記電子透かし検査手段による該コンテンツの検査結果に応じて該暗号化コンテンツのコピー動作を制御することを特徴とする情報処理装置。

【請求項４１】

コンテンツの外部機器へのコピー動作を実行する情報処理方法であって、

コピー対象となるコンテンツを読み込むステップと、

コピー対象となるコンテンツの識別情報を読み込むステップと、

コンテンツを直交変換する直交変換ステップと、

直交変換後のコンテンツを量子化及びハフマン符号化する符号化圧縮ステップ

と、

前記符号化圧縮されたコンテンツを暗号化する暗号化ステップと、

コピー対象となるコンテンツの識別情報とコンテンツの直交変換値又はそのハッシュ値を基に外部サーバに問合せを行うステップと、

該問合せ結果に応じて、該暗号化コンテンツのコピー動作を実行するか、又は、コンテンツ中に挿入された電子透かしの検査結果に応じて該暗号化コンテンツのコピー動作を制御するステップと、

を具備することを特徴とする情報処理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、画像や音楽などのコンテンツ中に、ほとんど目に見えない又は耳に聞こえない形で情報を埋め込む電子透かし技術に係り、特に、映像や音楽、放送番組などの各種コンテンツに埋め込まれた電子透かしを検査する電子透かし検査技術に関する。

【０００２】

更に詳しくは、本発明は、コンテンツに埋め込まれた電子透かしを検査した結果に従ってコンテンツの複製の可否を判断する電子透かし検査技術に係り、特に、計算負荷の高い電子透かし検査処理を代行して行う電子透かし検査技術に関する。

【０００３】

【従来の技術】

著作権とは、著作物を利用し得る相対的な排他的独占権であり、いわゆる無体財産権の１つに含まれる。ここで言う「著作物」とは、思想又は感情を創作的に表現したものであって、文芸、学術、美術又は音楽の範囲に属するものを指す。著作権は、各国の著作権法や、ベルヌ条約や万国著作権条約などの国際的な条約で保護されている。例えば、デジタル化されたテキストやコンピュータ・プログラム、デジタル化された音楽コンテンツ、映像コンテンツ、番組の放送コンテンツなど各種のメディアも著作物であり、著作権法制下で適正に保護を受けるべき

である。

【０００４】

著作権者自身においてのみ著作物の利用が行われるのはごく稀であり、他人が著作権を利用することに対して著作権者が一定の対価を得て許諾するというのが一般的である。したがって、著作権の保護を担保するためには、他人が勝手に（許可なく）著作物を複製するなどの著作物の不正使用を防止する必要がある。

【０００５】

著作権保護の歴史は１５世紀中ごろの印刷技術の発明に由来すると言われているが、昨今における電気・電子技術の飛躍的な進歩により著作物の複製が技術的に容易となってきているので、著作権をめぐる情勢も時々刻々と変貌してきている。

【０００６】

デジタル形式のデータやコンテンツの複製や改竄は極めて容易であり、著作権侵害の危険に無防備にさらされているとさえ言える。したがって、著作権法やその他の法規制を強化するだけでは不充分であり、情報技術の観点からも著作物の正当な利用を支援し若しくは不正利用を排除して、著作権の保護を拡充する必要があると思料される。

【０００７】

デジタル･コンテンツの世界において、不正コピーに対抗するための１つの手段として「電子透かし」（Digital Watermarking 又はData Hidingとも言う）と呼ばれる技術を挙げることができる。電子透かしとは、画像や音楽などのコンテンツ中に、ほとんど目に見えない又は耳に聞こえない形で情報を埋め込むことを意味する（例えば、「電子透かしを支えるデータ・ハイディング技術（上・下）」（日経エレクトロニクス１９９７年２月２４日号並びに同年３月１０日号）を参照のこと）。

【０００８】

電子透かしは、埋め込み先であるホスト信号の統計的性質を利用して、ホスト信号の一部に元の情報とは異なる情報を挿入することで実現される。例えば、著作権情報を電子透かしにより埋め込むことで、後にコンテンツを採取したときに

、透かしすなわち著作権情報を浮き上がらせて、データの流通経路や使用権の有無を検査したり、コピー制御情報を検証することができる。

【０００９】

例えば、デジタル音楽の著作権保護を目的として、１９９８年に米国大手レコード会社などが中心となってＳＤＭＩ（Secure Digital Music Interactive）なるフォーラムが設立された。ＳＤＭＩでは、ポータブル音楽プレーヤで著作権を保護する仕組みとして"Ｓｃｒｅｅｎｉｎｇ"という機能が規定されている。Ｓｃｒｅｅｎｉｎｇとは、ポータブル・デバイス（ＰＤ）のメモリ・レコーダ上にコピーしてよいコンテンツか否かを検査する仕組みであり、電子透かしを利用することが既に合意されている。例えば、不正に配信されたコンテンツや、既に１回（若しくは許容回数だけ）コピーされたコンテンツからはもはやコピーできないように、電子透かしによってＳｃｒｅｅｎｉｎｇをかけることができる。

【００１０】

図１には、ＳＤＭＩで想定しているＳｃｒｅｅｎｉｎｇ処理を行う機能ブロック図を模式的に示している。同図に示すように、ＣＤやＭＤのような記録メディアから読み取った音楽コンテンツ、あるいは通信媒体経由で受信した音楽コンテンツに対してまずＳｃｒｅｅｎｉｎｇにかけて（すなわち電子透かしを検査して）、コピー可能か否かをチェックした後、ＬＣＭ（Licensed SDMI Compliant Module）という仕組みで圧縮暗号化してから、携帯型機器（ＰＤ）上にコピーする。ここで言う、携帯型機器とは、圧縮暗号化されたデータ・コンテンツを伸張及び解読処理してコンテンツ再生する機能を持つポータブル・デバイス／プレーヤである。

【００１１】

図１に示すようなＳｃｒｅｅｎｉｎｇ処理システムは、例えば、パーソナル・コンピュータのような計算機システム上で実装され、携帯型機器との間は、例えば、ｉ－ｌｉｎｋ，ＵＳＢ（Universal Serial Bus）のような汎用バス・ケーブル、あるいはＩｒＤＡ（Infrared Data Association）やｂｌｕｅｔｏｏｔｈのような近接無線データ通信によって接続されている。

【００１２】

電子透かしは、音楽コンテンツ中に、耳に聞こえない程度に付加的なデータを挿入する技術であり、通常、約１５秒間に１２ビット程度のデータを挿入することができる。

【００１３】

ところで、電子透かしを検出するのには計算負荷が重く、時間がかかるという問題がある。例えば、音楽コンテンツ全体にわたって電子透かしを検査しようとすると、実演奏時間の１／２～１／３程度の計算時間を要してしまう。

【００１４】

ここで、上記のＳｃｒｅｅｎｉｎｇ処理をパーソナル・コンピュータ上で実装して、ＣＤから音楽コンテンツを携帯型機器上にコピーする場合について考察してみると、以下のような過程から構成される。すなわち、

【００１５】

（１）ＣＤからデータを読み出して、ハード・ディスク上にＷＡＶ形式（あるいは他のフォーマットでも可）ファイルとしてコピーする。

（２）ＷＡＶファイルを検査して、音楽データ全体にわたって電子透かしを検出する。

（３）電子透かしから”Ｎｏ　Ｍｏｒｅ　Ｃｏｐｙ”なるコピー禁止情報が検出されたなら、その時点で音楽コンテンツコピー処理を停止する。他方、かかるコピー禁止情報が検出されない場合には、楽曲の最後まで検出処理を継続して、最終的に検出されなかったら次のステップ（４）に進む。

（４）ＷＡＶファイルを例えばＡＴＲＡＣ３（Adaptive Transform Acoustic Coding 3）などで帯域圧縮する。

（５）帯域圧縮されたデータを暗号化して、ハード・ディスク上に一旦コピーする。

（６）ハード・ディスク上の圧縮暗号化ファイルを携帯型機器に転送する。

【００１６】

ここで、電子透かしが挿入されていない従来のＣＤからのコピーを試みた場合には、本来はＳｃｒｅｅｎｉｎｇにかけること自体意味がないにも拘わらず、上記のステップ（３）において、最終的にすべてのデータをチェックすることにな

ってしまい、検出時間に余分な時間がかかってしまう。例えば、ユーザが出かける前などに、急いでＣＤから携帯型機器に好きな音楽をコピーしたいような場合には、利便性を大いに損なう結果となる。

【００１７】

【発明が解決しようとする課題】

本発明の目的は、コンテンツに埋め込まれた電子透かしを検査することができる、優れた電子透かし検査技術を提供することにある。

【００１８】

本発明の更なる目的は、コンテンツに埋め込まれた電子透かしを検査した結果に従ってコンテンツの複製の可否を判断することができる、優れた電子透かし検査技術を提供することにある。

【００１９】

本発明の更なる目的は、計算負荷の高い電子透かし検査処理を代行して、コンテンツの複製の可否を判断し、コピー操作全体に要する時間を短縮することができる、優れた電子透かし検査技術を提供することにある。

【００２０】

【課題を解決するための手段】

本発明は、上記課題を参酌してなされたものであり、その第１の側面は、コンテンツの外部機器へのコピーを管理するコンテンツ・コピー管理システムであって、

コピー対象となるコンテンツを読み込む手段と、

コピー対象となるコンテンツの識別情報を読み込む手段と、

各コンテンツのコピー可否情報を保管するデータベースと、

コンテンツに挿入された電子透かしを検査する電子透かし検査手段と、

コンテンツの外部機器へのコピー動作を制御するコピー制御手段と、

を具備し、

前記コピー制御手段は、コピー対象となるコンテンツの識別情報及び／又は属性情報を基に前記データベースを検索し、該当するレコードが存在する場合にはそのレコードの内容に応じてコピー動作を制御し、該当するレコードが存在しな

い場合には前記電子透かし検査手段による該コンテンツの検査結果に応じてコピー動作を制御することを特徴とするコンテンツ・コピー管理システムである。

【００２１】

ここで、前記コピー制御手段は、コンテンツを圧縮及び暗号化してから前記外部機器にコピーするようにしてもよい。

【００２２】

また、前記コピー制御手段と前記データベースは安全な通信路を介して接続されていることが好ましい。安全な通信路は、例えば、電子認証や鍵交換の手続きを経て確立することができる。

【００２３】

また、本発明の第１の側面に係るコンテンツ・コピー管理システムは、さらに、コピー対象となるコンテンツの属性情報を取得する手段を備えていてもよい。

【００２４】

このような場合、前記属性情報は、コンテンツの一部を切り取ったデータであってもよい。あるいは、前記属性情報は、コンテンツの一部又は全部のハッシュ値であってもよい。前記属性情報は、コンテンツのエンベロープ値、リズムに相当する周期、スペクトルの広がり方などのコンテンツに関する特徴値又は特徴量であってもよい。

【００２５】

また、本発明の第２の側面は、コンテンツの外部機器へのコピーを管理するコンテンツ・コピー管理方法であって、

コピー対象となるコンテンツを読み込むステップと、

コピー対象となるコンテンツの識別情報を読み込むステップと、

コピー対象となるコンテンツの識別情報及び／又は属性情報を基にして各コンテンツのコピー可否情報を保管するデータベースに対して問い合わせるステップと、

該データベース中に該当するレコードが存在する場合にはそのレコードの内容に応じてコピー動作を制御するステップと、

該データベース中に該当するレコードが存在しない場合にはコンテンツ中に挿

入された電子透かしの検査結果に応じてコピー動作を制御するステップと、
を具備することを特徴とするコンテンツ・コピー管理方法である。

【００２６】

前記コピー動作を制御するステップでは、コンテンツを圧縮及び暗号化してから前記外部機器にコピーするようにしてもよい。

【００２７】

また、前記データベースへの問合せは安全な通信路を介して行われることが好ましい。安全な通信路は、例えば、電子認証や鍵交換の手続きを経て確立することができる。

【００２８】

また、本発明の第２の側面に係るコンテンツ・コピー管理方法は、さらに、コピー対象となるコンテンツの属性情報を取得するステップを備えていてもよい。このような場合、前記属性情報は、コンテンツの一部を切り取ったデータであってもよい。あるいは、前記属性情報は、コンテンツの一部又は全部のハッシュ値であってもよい。前記属性情報は、コンテンツのエンベロープ値、リズムに相当する周期、スペクトルの広がり方などのコンテンツに関する特徴値又は特徴量であってもよい。

【００２９】

また、本発明の第３の側面は、コンテンツの外部機器へのコピー動作を実行する情報処理装置であって、

コピー対象となるコンテンツを読み込む手段と、

コピー対象となるコンテンツの識別情報を読み込む手段と、

コンテンツに挿入された電子透かしを検査する電子透かし検査手段と、

コンテンツの外部機器へのコピー動作を制御するコピー制御手段と、
を具備し、

前記コピー制御手段は、コピー対象となるコンテンツの識別情報及び／又は属性情報を基に外部サーバに対して問合せを行い、該問合せ結果に応じて、コンテンツのコピー動作を実行するか、又は、前記電子透かし検査手段による該コンテンツの検査を実行して該検査結果に従ってコピー動作を制御することを特徴とす

る情報処理装置である。

【００３０】

前記コピー制御手段は、コンテンツを圧縮及び暗号化してから前記外部機器にコピーするようにしてもよい。

【００３１】

また、前記外部サーバとは安全な通信路を介して接続されていることが好ましい。安全な通信路は、例えば、電子認証や鍵交換の手続きを経て確立することができる。

【００３２】

また、本発明の第３の側面に係る情報処理装置は、さらに、コピー対象となるコンテンツの属性情報を取得する手段を備えていてもよい。このような場合、前記属性情報は、コンテンツの一部を切り取ったデータであってもよい。あるいは、前記属性情報は、コンテンツの一部又は全部のハッシュ値であってもよい。前記属性情報は、コンテンツのエンベロープ値、リズムに相当する周期、スペクトルの広がり方などのコンテンツに関する特徴値又は特徴量であってもよい。

【００３３】

また、本発明の第４の側面は、コンテンツの外部機器へのコピー動作を実行する情報処理方法であって、

コピー対象となるコンテンツを読み込むステップと、

コピー対象となるコンテンツの識別情報を読み込むステップと、

コピー対象となるコンテンツの識別情報及び／又は属性情報を基に外部サーバに対して問合せを行うステップと、

該問合せ結果に応じて、コンテンツのコピー動作を実行するか、又は、コンテンツに挿入された電子透かしの検査を実行して該検査結果に従ってコピー動作を制御するステップと、

を具備することを特徴とする情報処理方法である。

【００３４】

前記コピー動作を制御するステップでは、コンテンツを圧縮及び暗号化してから前記外部機器にコピーするようにしてもよい。

【００３５】

また、前記外部サーバへの問合せは安全な通信路を介して行うことが好ましい。安全な通信路は、例えば、電子認証や鍵交換の手続きを経て確立することができる。

【００３６】

また、本発明の第４の側面に係る情報処理方法は、さらに、コピー対象となるコンテンツの属性情報を取得するステップを備えていてもよい。このような場合、前記属性情報は、コンテンツの一部を切り取ったデータであってもよい。あるいは、前記属性情報は、コンテンツの一部又は全部のハッシュ値であってもよい。前記属性情報は、コンテンツのエンベロープ値、リズムに相当する周期、スペクトルの広がり方などのコンテンツに関する特徴値又は特徴量であってもよい。

【００３７】

また、本発明の第５の側面は、各コンテンツに関するコピー可否情報を管理するサーバであって、

コンテンツの識別情報及び／又は属性情報を基に検索可能なデータベースと、

コンテンツのコピー可否に関する問合せを受信する受信手段と、

該問合せに応答して前記データベースを検索する検索手段と、

前記データベースの検索結果を問い合わせ元に送信する送信手段と、

を具備することを特徴とするサーバである。

【００３８】

本発明の第５の側面に係るサーバは、問合せ元とは安全な通信路を介して接続されていることが好ましい。安全な通信路は、例えば、電子認証や鍵交換の手続きを経て確立することができる。

【００３９】

また、前記属性情報は、コンテンツの一部を切り取ったデータであってもよい。あるいは、前記属性情報は、コンテンツの一部又は全部のハッシュ値であってもよい。前記属性情報は、コンテンツのエンベロープ値、リズムに相当する周期、スペクトルの広がり方などのコンテンツに関する特徴値又は特徴量であってもよい。

【００４０】

また、本発明の第６の側面は、コンテンツの外部機器へのコピーを管理する処理をコンピュータ・システム上で実行するためのコンピュータ・ソフトウェアをコンピュータ可読形式で物理的に格納したソフトウェア記憶媒体であって、前記コンピュータ・ソフトウェアは、

コピー対象となるコンテンツを読み込むステップと、

コピー対象となるコンテンツの識別情報を読み込むステップと、

コピー対象となるコンテンツの属性情報を取得するステップと、

コピー対象となるコンテンツの識別情報及び／又は属性情報を基にして各コンテンツのコピー可否情報を保管するデータベースに対して問い合わせるステップと、

該データベース中に該当するレコードが存在する場合にはそのレコードの内容に応じてコピー動作を制御するステップと、

該データベース中に該当するレコードが存在しない場合にはコンテンツ中に挿入された電子透かしの検査結果に応じてコピー動作を制御するステップと、

を具備することを特徴とするソフトウェア記憶媒体である。

【００４１】

また、本発明の第７の側面は、コンテンツの外部機器へのコピーを実行する処理をコンピュータ・システム上で実行するためのコンピュータ・ソフトウェアをコンピュータ可読形式で物理的に格納したソフトウェア記憶媒体であって、前記コンピュータ・ソフトウェアは、

コピー対象となるコンテンツを読み込むステップと、

コピー対象となるコンテンツの識別情報を読み込むステップと、

コピー対象となるコンテンツの属性情報を取得するステップと、

コピー対象となるコンテンツの識別情報及び／又は属性情報を基に外部サーバに対して問合せを行うステップと、

該問合せ結果に応じて、コンテンツのコピー動作を実行するか、又は、コンテンツに挿入された電子透かしの検査を実行して該検査結果に従ってコピー動作を制御するステップと、

を具備することを特徴とするソフトウェア記憶媒体である。

【００４２】

本発明の第６及び第７の各側面に係るソフトウェア記憶媒体は、例えば、様々なプログラム･コードを実行可能な汎用コンピュータ･システムに対して、コンピュータ・ソフトウェアをコンピュータ可読な形式で提供する媒体である。このような媒体は、例えば、ＣＤ（Compact Disc）やＦＤ（Floppy Disk）、ＭＯ（Magneto-Optical disc）などの着脱自在で可搬性の記憶媒体である。あるいは、ネットワーク（ネットワークは無線、有線の区別を問わない）などの伝送媒体などを経由してコンピュータ・ソフトウェアを特定のコンピュータ・システムに提供することも技術的に可能である。

【００４３】

このようなソフトウェア記憶媒体は、コンピュータ・システム上で所定のコンピュータ・ソフトウェアの機能を実現するための、コンピュータ・ソフトウェアと記憶媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、本発明の第６及び第７の側面に係るソフトウェア記憶媒体を介して所定のコンピュータ・ソフトウェアをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の第１、第２、並びに、第３、第４の各側面に係るコンテンツ・コピー管理システム及び方法、並びに、情報処理装置及び方法と同様の作用効果を得ることができる。

【００４４】

また、本発明の第８の側面は、コンテンツの外部機器へのコピーを管理するコンテンツ・コピー管理システムであって、

コピー対象となるコンテンツを読み込む手段と、

コピー対象となるコンテンツの識別情報を読み込む手段と、

各コンテンツのコピー可否情報を保管するデータベースと、

コンテンツに挿入された電子透かしを検査する電子透かし検査手段と、

コンテンツを直交変換する直交変換手段と、

直交変換後のコンテンツを量子化及びハフマン符号化する符号化圧縮手段と、

前記符号化圧縮されたコンテンツを暗号化する暗号化手段と、

コンテンツの外部機器への該暗号化コンテンツのコピー動作を制御するコピー制御手段と、

を具備し、

前記コピー制御手段は、コピー対象となるコンテンツの識別情報とコンテンツの直交変換値又はそのハッシュ値を基に前記データベースを検索し、該当するレコードが存在する場合にはそのレコードの内容に応じて該暗号化コンテンツのコピー動作を制御し、該当するレコードが存在しない場合には前記電子透かし検査手段による該コンテンツの検査結果に応じて該暗号化コンテンツのコピー動作を制御することを特徴とするコンテンツ・コピー管理システムである。ここで言う「直交変換」には、例えばｍＤＣＴ（変形離散コサイン変換）や、ＤＣＴ（離散コサイン変換）、ｗａｖｅｌｅｔ（”ｗａｖｅｌｅｔ”は米サマス・テクノロジーズ社が開発した波形分析技術）などが含まれる（以下、同様）。

【００４５】

また、本発明の第９の側面は、コンテンツの外部機器へのコピーを管理するコンテンツ・コピー管理方法であって、

コピー対象となるコンテンツを読み込むステップと、

コピー対象となるコンテンツの識別情報を読み込むステップと、

コンテンツを直交変換する直交変換ステップと、

直交変換後のコンテンツを量子化及びハフマン符号化する符号化圧縮ステップと、

前記符号化圧縮されたコンテンツを暗号化する暗号化ステップと、

コピー対象となるコンテンツの識別情報とコンテンツの直交変換値又はそのハッシュ値を基にして各コンテンツのコピー可否情報を保管するデータベースに対して問い合わせるステップと、

該データベース中に該当するレコードが存在する場合にはそのレコードの内容に応じて該暗号化コンテンツのコピー動作を制御するステップと、

該データベース中に該当するレコードが存在しない場合にはコンテンツ中に挿入された電子透かしの検査結果に応じて該暗号化コンテンツのコピー動作を制御するステップと、

を具備することを特徴とするコンテンツ・コピー管理方法である。

【００４６】

また、本発明の第１０の側面は、コンテンツの外部機器へのコピー動作を実行する情報処理装置であって、

コピー対象となるコンテンツを読み込む手段と、

コピー対象となるコンテンツの識別情報を読み込む手段と、

コンテンツに挿入された電子透かしを検査する電子透かし検査手段と、

コンテンツを直交変換する直交変換手段と、

直交変換後のコンテンツを量子化及びハフマン符号化する符号化圧縮手段と、

前記符号化圧縮されたコンテンツを暗号化する暗号化手段と、

コンテンツの外部機器への該暗号化コンテンツのコピー動作を制御するコピー制御手段と、

を具備し、

前記コピー制御手段は、コピー対象となるコンテンツの識別情報とコンテンツの直交変換値又はそのハッシュ値を基に外部サーバに問合せを行い、該問合せ結果に応じて、該暗号化コンテンツのコピー動作を実行するか、又は、前記電子透かし検査手段による該コンテンツの検査結果に応じて該暗号化コンテンツのコピー動作を制御することを特徴とする情報処理装置である。

【００４７】

また、本発明の第１１の側面は、コンテンツの外部機器へのコピー動作を実行する情報処理方法であって、

コピー対象となるコンテンツを読み込むステップと、

コピー対象となるコンテンツの識別情報を読み込むステップと、

コンテンツを直交変換する直交変換ステップと、

直交変換後のコンテンツを量子化及びハフマン符号化する符号化圧縮ステップと、

前記符号化圧縮されたコンテンツを暗号化する暗号化ステップと、

コピー対象となるコンテンツの識別情報とコンテンツの直交変換値又はそのハッシュ値を基に外部サーバに問合せを行うステップと、

該問合せ結果に応じて、該暗号化コンテンツのコピー動作を実行するか、又は、コンテンツ中に挿入された電子透かしの検査結果に応じて該暗号化コンテンツのコピー動作を制御するステップと、
を具備することを特徴とする情報処理方法である。

【００４８】

【作用】

本発明では、コンテンツの複製を行う計算機システム自体がスクリーニング（Ｓｃｒｅｅｎｉｎｇ）すなわち電子透かしの検出を必ずしも行わず、別の手段により、コンテンツのコピー制御情報を取得できるようにした。例えば、コンテンツには電子透かしが挿入されていないことがあらかじめ分かっているＣＤからコピーするような場合には、かかるＣＤであることを確認できれば、電子透かしの検出処理そのものをスキップして、コピー操作全体の所要時間を短縮化することができる。

【００４９】

すなわち、本発明によれば、データから電子透かしを検出する必要がないので処理時間が短縮化され、ユーザの利便性が向上する。

【００５０】

また、電子透かしを検出する場合であっても、コンテンツ（例えば楽曲）全体にわたって検出する必要がないので、処理時間が短縮化され、ユーザの利便性が向上する。

【００５１】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００５２】

【発明の実施の形態】

以下、図面を参照しながら本発明の実施例を詳解する。

【００５３】

図２には、本発明の実施例に係るコンテンツ・コピー管理システム１の全体構成を模式的に示している。

【００５４】

このコンテンツ・コピー管理システム１は、音楽などのコンテンツを携帯型機器２０にコピーする情報処理端末１０と、情報処理端末１０に対してコンテンツに関する電子透かし検出処理の代行業務を提供するサーバ３０とで構成される。ここで言う、携帯型機器とは、圧縮暗号化されたデータ・コンテンツを伸張及び解読処理してコンテンツ再生する機能を持つポータブル・デバイス／プレーヤである。

【００５５】

情報処理端末１０は、例えば、家庭内に設置されるパーソナル・コンピュータ（ＰＣ）上に所定のアプリケーションを起動するという形態で実現される（後述）。パーソナル・コンピュータは、例えば米ＩＢＭ社のＰＣ／ＡＴ互換機及びその後継機である。

【００５６】

情報処理端末１０は、サーバ３０とは認証を行い、安全な通信路が確保されているものとする。

【００５７】

情報処理端末１０は、ＣＤ－ＲＯＭドライブ（図示しない）に装填したＣＤから音楽データを読み出して、携帯型機器２０へのコピーを行う。

【００５８】

ＣＤから読み出した音楽データは、ハード・ディスク（図示しない）上にＷＡＶ形式ファイルとして一時保存される。

【００５９】

また、ＣＤからの音楽データ読み出しの際に、楽曲に対して一意に割当られる識別情報ＩＳＲＣ（International Standard Recording Code）を、ＴＯＣ（Table Of Contents）領域から取り出す。

【００６０】

音楽データを他の機器やメディアにコピーする際にＳｃｒｅｅｎｉｎｇすなわち電子透かし情報の検査を行うことがＳＤＭＩ（Secure Digital Music Interactive）により規定されている（前述）。但し、本実施例では、情報処理端末１０

は、Ｓｃｒｅｅｎｉｎｇ処理を開始する前に、サーバ３０に対して電子透かし情報の問合せを行う。この問合せには、対象となる楽曲のＩＳＲＣ（又はコンテンツを識別可能なその他の情報）を含ませておく。

【００６１】

サーバ３０は、各楽曲に関する電子透かし情報をデータベース管理しており、ＩＳＲＣで各楽曲のエントリを検索することができるようになっている。したがって、情報処理端末１０側から問合せを受け取ると、それに含まれているＩＳＲＣを基に、当該楽曲のエントリの照合を試みる。そして、照合結果を要求元の情報処理端末１０側に戻す。

【００６２】

問合せに対する応答を受け取った情報処理端末１０は、その照合結果に応じて処理を進める。例えば、電子透かし入りのメディアでない旨の結果を受け取った場合には、Ｓｃｒｅｅｎｉｎｇを行っても意味がないので、電子透かしの検出処理をスキップして、携帯型機器への音楽コンテンツのコピーを開始することができる。

【００６３】

また、上述のようにＩＳＲＣを用いる場合、情報処理端末１０上でＣＤ－ＲＯＭドライブからＩＳＲＣを読み出す際に、途中の経路を改竄して、電子透かし入りでない別のＩＳＲＣ（又はコピー可であることが既に分かっている別のＣＤのＩＳＲＣ）と置換されてしまう危険がある。そこで、サーバ３０に対する問合せにＩＳＲＣだけでなく、例えば全体の演奏時間などメディア上のデータ・コンテンツ自体に関する他の情報を付加するようにして、なりすましの危険を排除することもできる。但し、ＩＳＲＣなどの識別情報が、メディアから安全に取得する技術が存在するならば、このような属性情報を送信しなくてもよい。

【００６４】

また、音楽の一部を切りとってそのデータをサーバ３０に送ったり、さらに楽曲中の２以上の場所からサンプリングして、それらをサーバ３０に送って照合するということも可能である。サンプルする場所を毎回ランダムに変更して特定できないようにすることで、なりすましを排除することができる。

【００６５】

また、音楽のサンプルを直接照合しようとすると比較的大きなデータ量になる可能性があり、通信負荷を増大させてしまいかねない。そこで、音楽データの一部又は全部を攪乱したハッシュ値をとり、その値をサーバ３０側に転送して照合することで電子透かしの有無を確認するようにしてもよい。（ハッシュ関数は、デジタル署名などにも利用されるものであり、ハッシュ関数にいれるデータの一部でも改竄された場合には結果が大きく異なる性質を持つので、推測が難しく、容易に改竄を検出することができる。また、一方向性関数の特性を有するので、結果に合わせた改竄も難しい（周知）。）

【００６６】

あるいは、音楽データ中から特定の特徴値または特徴量を演算して、これをサーバ３０において照合する手法も挙げられる。例えば、エンベロープ値であるとか、リズムに相当する周期であるとか、スペクトルの広がり方であるとかのデータを分析して、このような演算結果をサーバ３０側に転送して照合するようにしてもよい。

【００６７】

図２に示すようなコンテンツ・コピー管理システム１の構成及び動作特性によれば、情報処理端末１０においてＣＤから携帯型機器２０に音楽コンテンツをコピーする場合において、そもそも電子透かしを含まないＣＤに対する電子透かし検出処理が省略されるので、利便性が高まる。

【００６８】

次いで、本発明の第１の実施形態に係るコンテンツ・コピー管理システム１において、情報処理端末１０上でＣＤ上の音楽データを携帯型機器２０にコピーするときの処理手順について説明する。上述したように、この実施形態によれば、情報処理端末１０は、サーバ３０側のデータベースに対して問合せを行うことによって、電子透かしの検出処理を省略することができる。

【００６９】

図３には、情報処理端末１０上で実行する処理手順をフローチャートの形式で示している。以下、このフローチャートに従って説明する。

【００７０】

まず、ＣＤ－ＲＯＭドライブ（図示しない）に装填されたＣＤから、ＩＳＲＣ（International Standard Recording Code）若しくはこれと同等のコンテンツ識別情報を取得する（ステップＳ１）。

【００７１】

一般に、ＣＤにはＴＯＣ（Table Of Contents）のようなデータ領域が確保されており、ＩＳＲＣやその他のコンテンツ属性情報を記録できるようになっている。ＩＳＲＣは、１２桁の数字及びアルファベット文字で構成された、ＣＤのタイトル毎に割り振られる固有の識別情報である。

【００７２】

次いで、ＣＤから所望の楽曲データを読み込んで、端末１０内のハード・ディスク（図示しない）にコピーしておく（ステップＳ２）。

【００７３】

次いで、ハード・ディスク上の楽曲データから、その属性情報を取得する（ステップＳ３）。ここで言う属性情報とは、例えば、楽曲全体の演奏時間や、楽曲から演算して取り出した特定の特徴値（量）などである。特徴値は、エンベロープ値やリズムに相当する周期、スペクトルの広がり方などの分析値などでよい。かかる属性情報は、ＩＳＲＣ以外の補完的な識別情報として用いられ、不正ユーザによる「なりすまし」を防止することができる。但し、ＩＳＲＣなどの識別情報をメディアから安全に取り出す手法が確立されている場合には、属性情報を使用する必要はない。

【００７４】

次いで、問合せ先となるサーバ３０と接続し（ステップＳ４）、さらにサーバ３０と認証及び鍵交換を行うことにより（ステップＳ５）、サーバ３０との安全な通信路を確保する。

【００７５】

認証には、共通鍵あるいは公開鍵を用いた認証方式を採用することができるが、そのプロトコルはＩＳＯ（International Organization for Standardization）で既に標準化されている。一方の装置から認証の要求を発行する際に乱数列も

送出し、他方の装置はその乱数を所定の鍵で暗号化して返信する。一方の装置では、これを所定の鍵で解き、元の乱数と一致するかどうかを見ることで、相手が共通の鍵又は信頼できる鍵を保持しているか、言い換えれば正しい相手か否かを認証することができる。

【００７６】

安全な通信路が確立した後、情報処理端末１０は、ステップＳ１において読み込んだＩＳＲＣコードと、ステップＳ３において取得した属性情報とをサーバ３０側に転送して、ＣＤの調査を要求する（ステップＳ６）。

【００７７】

ＣＤ調査要求に対して、サーバ３０側では、ＩＳＲＣコードを基に自身のデータベースを検索して、そのレコードが存在するか、さらには属性情報が一致するか否かを判別して、その結果を情報処理端末１０側に返す（ステップＳ７）。但し、サーバ３０側で行う処理については、後に詳解する。

【００７８】

情報処理端末１０側では、サーバ３０側からの返答を基に、楽曲データの携帯型機器２０へのコピーが許されるか否かを判別する。

【００７９】

返答内容が、データベース中に該当するレコードが存在することを示していれば（ステップＳ８）、装填中のＣＤはデータベース登録されたものであり、電子透かしにより挿入されたデータは既知であるから、Ｓｃｒｅｅｎｉｎｇすなわち電子透かしの検出処理を省略することができる。この場合、ＣＤからのコピーの可否判断のみを行う（ステップＳ９、Ｓ１０）。登録ＣＤは１回のみコピーが許容されているとすれば、ステップＳ９において、装填中のメディアがＣＤ－Ｒか否かをチェックすればよい。

【００８０】

コピー可能であれば、ステップＳ９１に進んで、ＬＣＭによる楽曲データの圧縮（ＡＴＲＡＣ３による帯域圧縮）及び暗号化を行ってから、携帯型機器２０へのコピーを行う。これに対し、コピー不可であれば、ステップＳ９２に進み、コピー処理を中止する。

【００８１】

他方、ステップＳ８において、サーバ３０側のデータベースに該当レコードが存在しない、すなわち装填中のＣＤが登録ＣＤではないと判定された場合には、Ｓｃｒｅｅｎｉｎｇすなわち電子透かし検出処理を行うより他ない（ステップＳ１３）。

【００８２】

電子透かし検出を行いコピーの可否を判断した結果、コピー可能であればＬＣＭによる楽曲の圧縮（ＡＴＲＡＣ３などによる帯域圧縮）及び暗号化を行ってから、携帯型機器２０へのコピーを行う（ステップＳ１４→Ｓ１１）。また、コピー不可であれば、ステップＳ１５に進み、コピー処理を中止する。

【００８３】

なお、音楽データを読み出すＣＤ－ＲＯＭドライブが充分信用できるものである場合（あるエンティティにより所定の安全性を保つことが認定されている場合など）、該ドライブと情報処理端末１０本体が認証及び鍵交換を行うことにより、ＩＳＲＣデータや正常なＣＤであることが安全に通知できる仕組みを備えていることがより好ましい。

【００８４】

また、図４には、図３に示すような処理手順を実行する情報処理端末１０からの問合せに対するサーバ３０側が行う処理手順をフローチャートの形式で示している。以下、このフローチャートに従って説明する。

【００８５】

まず、クライアントすなわち情報処理端末１０側からの接続要求に応答して（ステップＳ２１）、接続処理を行う（ステップＳ２２）。さらに、情報処理端末１０と認証及び鍵交換を行うことにより（ステップＳ２３）、情報処理端末１０との安全な通信路を確保する（同上）。

【００８６】

次いで、情報処理端末１０側から送られてくる照合データを受信する（ステップＳ２４）。照合データには、楽曲に関するＩＳＲＣコードと属性情報が含まれている。また、ここで言う属性情報とは、楽曲全体の演奏時間や、エンベロープ

値やリズムに相当する周期、スペクトルの広がり方などの分析値などの楽曲から取り出された特徴値である。

【００８７】

サーバ３０は、受信データ中にＩＳＲＣが含まれているか否かをチェックして（ステップＳ２５）、ＩＳＲＣが含まれる場合にはＩＳＲＣからデータベースを検索し（ステップＳ２６）、含まれていなければデータベースを全数一致検索して、特徴値などの属性情報が一致するレコードを探し出す（ステップＳ２７）。

【００８８】

データベースを検索した結果、照合データと一致するレコードがデータベース中から発見できたか否かを判別する（ステップＳ２８）。

【００８９】

一致するレコードが存在する場合には、付加データを付けてその旨を情報処理端末１０側に返す（ステップＳ２９）。付加データには、コピー制御情報（例えば「ＣＤ－Ｒからのコピー不可」など）を含めることができる。

【００９０】

他方、一致するレコードが存在しない場合には、その旨を情報処理端末１０側に返す（ステップＳ３０）。

【００９１】

そして、情報処理端末１０との接続を解除して（ステップＳ３１）、本処理ルーチン全体を終了する。

【００９２】

図３及び図４に示す例では、情報処理端末１０は、サーバ３０側に対して装填中のＣＤが登録済みＣＤであるか否かのみを問合せ、コピー可能であるか否かは情報処理端末１０側で判断するようになっている（図３のステップＳ９及びＳ１０）。これに対し、サーバ３０は、情報処理端末１０側からの問合せに応答して、さらにコピーの可否まで判断して返答することもできる。

【００９３】

図５及び図６には、後者の場合における情報処理端末１０及びサーバ３０側が行う処理手順をそれぞれフローチャートの形式で示している。以下、これらフロ

ーチャートに従って説明する。

【００９４】

情報処理端末１０側では、まず、ＣＤ－ＲＯＭドライブ（図示しない）に装填されたＣＤから、ＩＳＲＣ（International Standard Recording Code）若しくはこれと同等のコンテンツ識別情報を取得する（ステップＳ４１）。

【００９５】

次いで、ＣＤから所望の楽曲データを読み込んで、端末１０内のハード・ディスク（図示しない）にコピーしておく（ステップＳ４２）。

【００９６】

次いで、ハード・ディスク上の楽曲データから、その属性情報を取得する（ステップＳ４３）。ここで言う属性情報とは、例えば、楽曲全体の演奏時間や、楽曲から演算して取り出した特定の特徴値（量）などである。特徴値は、エンベロープ値やリズムに相当する周期、スペクトルの広がり方などの分析値などでよい。かかる属性情報は、ＩＳＲＣ以外の補完的な識別情報として用いられ、不正ユーザによる「なりすまし」を防止することができる。但し、ＩＳＲＣのような識別情報をメディアから安全に引き出す手法が確立されていれば、このような属性情報を使用する必要はない。

【００９７】

次いで、問合せ先となるサーバ３０と接続し（ステップＳ４４）、さらにサーバ３０と認証及び鍵交換を行うことにより（ステップＳ４５）、サーバ３０との安全な通信路を確保する。

【００９８】

そして、情報処理端末１０は、ＩＳＲＣコード及び属性情報をサーバ３０側に転送して、コピー可否の判断を要求する（ステップＳ４６）。判断のために、装填中のＣＤがＣＤ－Ｒか否かなどの付随情報も併せて送信する。

【００９９】

コピー可否の判断要求に対して、サーバ３０側では、ＩＳＲＣコードを基に自身のデータベースを検索して、そのレコードが存在するか、さらには属性情報が一致するか否かなどを判別して、判断結果を情報処理端末１０側に返す（ステッ

プＳ４７）。但し、サーバ３０側で行う処理については、後に詳解する。

【０１００】

情報処理端末１０側では、サーバ３０側からの返答を基に、楽曲データの携帯型機器２０へのコピーが許されるか否かを判別する（ステップＳ４８）。

【０１０１】

サーバ３０による判断結果が「コピー可」であれば、ステップＳ４９に進んで、ＬＣＭによる楽曲の圧縮及び暗号化を行ってから、携帯型機器２０へのコピーを行う。

【０１０２】

また、サーバ３０による判断結果が「コピー不可」であれば、ステップＳ５０に進み、コピー処理を中止する。

【０１０３】

また、サーバ３０による判断結果が「Ｓｃｒｅｅｎｉｎｇ実行」であれば、電子透かし検出処理を行う他ない（ステップＳ５１）。電子透かし検出を行いコピーの可否を判断した結果、コピー可能であればＬＣＭによる楽曲の圧縮（ＡＴＲＡＣ３などによる帯域圧縮）及び暗号化を行ってから、携帯型機器２０へのコピーを行う（ステップＳ５２→Ｓ４９）。また、コピー不可であれば、ステップＳ５３に進み、コピー処理を中止する。

【０１０４】

他方、サーバ３０側では、クライアントすなわち情報処理端末１０側からの接続要求に応答して（ステップＳ６１）、接続処理を行う（ステップＳ６２）。さらに、情報処理端末１０と認証及び鍵交換を行うことにより（ステップＳ６３）、情報処理端末１０との安全な通信路を確保する。

【０１０５】

次いで、情報処理端末１０側から送られてくる照合データを受信する（ステップＳ６４）。照合データには、楽曲に関するＩＳＲＣコードと属性情報が含まれている。また、ここで言う属性情報とは、楽曲全体の演奏時間や、エンベロープ値やリズムに相当する周期、スペクトルの広がり方などの分析値などの楽曲から取り出された特徴値である。また、情報処理端末１０において現在装填中のＣＤ

がＣＤ－Ｒか否かなどの付随データも併せて受信する。

【０１０６】

サーバ３０は、受信データ中にＩＳＲＣが含まれているか否かをチェックして（ステップＳ６５）、ＩＳＲＣが含まれる場合にはＩＳＲＣからデータベースを検索し（ステップＳ６６）、含まれていなければデータベースを全数一致検索して、特徴値などの属性情報が一致するレコードを探し出す（ステップＳ６７）。

【０１０７】

データベースを検索した結果、照合データと一致するレコードがデータベース中から発見できたか否かを判別する（ステップＳ６８）。

【０１０８】

一致するレコードが存在する場合には、レコード内の記述などを基に、ＣＤからのコピーの可否を判断する（ステップＳ６９）。また、情報処理端末１０側から送られてきた、「ＣＤ－Ｒか否か」などの付加データを参考にしてコピーの可否を判断してもよい。

【０１０９】

コピー可能であれは、情報処理端末１０に対して「コピー可」を返し（ステップＳ７０）、コピー不可であれば、情報処理端末に対して「コピー不可」を返す（ステップＳ７２）。

【０１１０】

また、データベース上にレコードが存在しない場合には（ステップＳ６８）、情報処理端末１０においてＳｃｒｅｅｎｉｎｇ処理を省略することは許されないので、情報処理端末に対して「Ｓｃｒｅｅｎｉｎｇ実行」を返す（ステップＳ７３）。

【０１１１】

そして、情報処理端末１０との接続を解除して（ステップＳ７１）、本処理ルーチン全体を終了する。

【０１１２】

図７には、サーバ３０側のデータベースに対して問合せを行うことによって電子透かし検出処理を省略するための、情報処理端末１０上で実行する処理手順の

さらに他の例をフローチャートの形式で示している。

【０１１３】

データベースに対する照合処理のために、ＩＳＲＣしか使用しない場合には、ＣＤ－ＲＯＭドライブからＩＳＲＣを読み出す際に、途中の経路を改竄して、電子透かし入りでない別のＩＳＲＣ（又はコピー可であることが分かっている別のＣＤのＩＳＲＣ）と置換されてしまう危険がある。そこで、図７に示す例では、楽曲のデータの一部を参照することで、ＣＤであるか否かを照合するようにしている。以下、フローチャートに従って説明する。

【０１１４】

まず、ＣＤ－ＲＯＭドライブ（図示しない）に装填されたＣＤから、ＩＳＲＣ（International Standard Recording Code）若しくはこれと同等のコンテンツ識別情報を取得する（ステップＳ８１）。

【０１１５】

次いで、ＣＤから所望の楽曲データを読み込んで、端末１０内のハード・ディスク（図示しない）にコピーしておく（ステップＳ８２）。

【０１１６】

次いで、ハード・ディスク上の楽曲データから、ランダムに１箇所又は数カ所のデータをある秒数だけ選択して実データを取り出すとともに、そのデータ位置情報（先頭から何バイト目か、あるいは演奏時間上何秒目かなど）を、属性情報取得する（ステップＳ８３）。実データを取り出す場所は固定であってもよいが、不正ユーザによるデータ置換の危険を排除するにはランダムな場所であることが好ましい。

【０１１７】

次いで、問合せ先となるサーバ３０と接続し（ステップＳ８４）、さらにサーバ３０と認証及び鍵交換を行うことにより（ステップＳ８５）、サーバ３０との安全な通信路を確保する。

【０１１８】

そして、情報処理端末１０は、ステップＳ８１において読み込んだＩＳＲＣコードと、ステップＳ８３において取得した属性情報とをサーバ３０側に転送して

、ＣＤの調査を要求する（ステップＳ８６）。

【０１１９】

ＣＤ調査要求に対して、サーバ３０側では、ＩＳＲＣコードを基に自身のデータベースを検索して、そのレコードが存在するか、さらには属性情報（すなわち楽曲の一部を切り出したデータ）が一致するか否かを判別して、その結果を情報処理端末１０側に返す（ステップＳ８７）。調査要求に対してサーバ３０側において実行すべき処理手順は、属性情報ではなく切り出した実データの一部をデータベースで照合するという点以外は図４に示したものと同様なので、ここでは説明を省略する。

【０１２０】

情報処理端末１０側では、サーバ３０側からの返答を基に、楽曲データの携帯型機器２０へのコピーが許されるか否かを判別する。

【０１２１】

返答内容が、データベース中に該当するレコードが存在することを示していれば（ステップＳ８８）、装填中のＣＤはデータベース登録されたものであり、電子透かしにより挿入されたデータは既知であるから、Ｓｃｒｅｅｎｉｎｇすなわち電子透かしの検出処理を省略することができる。この場合、ＣＤからのコピーの可否判断のみを行う（ステップＳ８９、Ｓ９０）。登録ＣＤは１回のみコピーが許容されているとすれば、ステップＳ８９において、装填中のメディアがＣＤ－Ｒか否かをチェックすればよい。

【０１２２】

コピー可能であれば、ステップＳ９１に進んで、ＬＣＭによる楽曲データの圧縮（ＡＴＲＡＣ３による帯域圧縮）及び暗号化を行ってから、携帯型機器２０へのコピーを行う。これに対し、コピー不可であれば、ステップＳ１２に進み、コピー処理を中止する。

【０１２３】

他方、ステップＳ８８において、サーバ３０側のデータベースに該当レコードが存在しない、すなわち装填中のＣＤが登録ＣＤではないと判定された場合には、Ｓｃｒｅｅｎｉｎｇすなわち電子透かし検出処理を行うより他ない（ステップ

Ｓ９３）。

【０１２４】

電子透かし検出を行いコピーの可否を判断した結果、コピー可能であればＬＣＭによる楽曲の圧縮（ＡＴＲＡＣ３などによる帯域圧縮）及び暗号化を行ってから、携帯型機器２０へのコピーを行う（ステップＳ９４→Ｓ９１）。また、コピー不可であれば、ステップＳ９５に進み、コピー処理を中止する。

【０１２５】

図８には、サーバ３０側のデータベースに対して問合せを行うことによって電子透かし検出処理を省略するための、情報処理端末１０上で実行する処理手順のさらに他の例をフローチャートの形式で示している。

【０１２６】

図８に示す例では、楽曲のデータの全部（又は一部でも可）をハッシュ関数にかけて得られたハッシュ値を参照することで、ＣＤであるか否かを照合するようにしている。

【０１２７】

ここで、ハッシュ関数とは、データ列を圧縮して別のデータ列に置き換えるものである。一般に、ハッシュ関数に入れるデータの一部でも改竄された場合には結果が大きく異なる性質を持つので、推測が難しく、容易に改竄を検出することができる。また、一方向性関数の特性を有するので、結果に合わせた改竄も難しい（周知）。現在、ＳＨＡ－１と呼ばれるアルゴリズムが公開されている。

【０１２８】

以下、図８に示すフローチャートに従って説明する。

【０１２９】

まず、ＣＤ－ＲＯＭドライブ（図示しない）に装填されたＣＤから、ＩＳＲＣ（International Standard Recording Code）若しくはこれと同等のコンテンツ識別情報を取得する（ステップＳ１０１）。

【０１３０】

次いで、ＣＤから所望の楽曲データを読み込んで、端末１０内のハード・ディスク（図示しない）にコピーしておく（ステップＳ１０２）。

【０１３１】

次いで、ハード・ディスク上の楽曲データ全体をハッシュ関数にかけてそのハッシュ値を計算して、これを属性情報として一時的に保持する（ステップＳ１０３）。

【０１３２】

次いで、問合せ先となるサーバ３０と接続し（ステップＳ１０４）、さらにサーバ３０と認証及び鍵交換を行うことにより（ステップＳ１０５）、サーバ３０との安全な通信路を確保する。

【０１３３】

そして、情報処理端末１０は、ステップＳ１０１において読み込んだＩＳＲＣコードと、ステップＳ１０３において計算したハッシュ値とをサーバ３０側に転送して、ＣＤの調査を要求する（ステップＳ１０６）。

【０１３４】

ＣＤ調査要求に対して、サーバ３０側では、ＩＳＲＣコードを基に自身のデータベースを検索して、そのレコードが存在するか、さらにはそのハッシュ値が一致するか否かを判別して、その結果を情報処理端末１０側に返す（ステップＳ１０７）。

【０１３５】

図８に示す例ではデータ全体のハッシュ値をサーバ３０に送信して照合するので、図７に示した場合とは相違し、楽曲全体にわたって改竄されていないかどうかを検査することができ、ＣＤのデータに対してすげ替えやその他の何らかの不正な処理が印加されていないかどうかを確認することができる。また、ハッシュ値を送るので、楽曲全体にわたるデータを送信するための通信負荷が軽くて済む。サーバ３０側でも、楽曲全体ではなくそのハッシュ値だけを保管しておけばよいので、記憶容量を節約することができる。例えばＳＨＡ－１では、５１２ビットごとに１６０ビットのデータを出力するようになっているので、これを累積計算することで、楽曲全体のハッシュ値を得ることができる。

【０１３６】

情報処理端末１０側では、サーバ３０側からの返答を基に、楽曲データの携帯

型機器２０へのコピーが許されるか否かを判別する。

【０１３７】

返答内容が、データベース中に該当するレコードが存在することを示していれば（ステップＳ１０８）、装填中のＣＤはデータベース登録されたものであり、電子透かしにより挿入されたデータは既知であるから、Ｓｃｒｅｅｎｉｎｇすなわち電子透かしの検出処理を省略することができる。この場合、ＣＤからのコピーの可否判断のみを行う（ステップＳ１０９、Ｓ１１０）。登録ＣＤは１回のみコピーが許容されているとすれば、ステップＳ１０９において、装填中のメディアがＣＤ－Ｒか否かをチェックすればよい。

【０１３８】

コピー可能であれば、ステップＳ１１１に進んで、ＬＣＭによる楽曲データの圧縮（ＡＴＲＡＣ３による帯域圧縮）及び暗号化を行ってから、携帯型機器２０へのコピーを行う。これに対し、コピー不可であれば、ステップＳ１１２に進み、コピー処理を中止する。

【０１３９】

他方、ステップＳ１０８において、サーバ３０側のデータベースに該当レコードが存在しない、すなわち装填中のＣＤが登録ＣＤではないと判定された場合には、Ｓｃｒｅｅｎｉｎｇすなわち電子透かし検出処理を行うより他ない（ステップＳ１１３）。

【０１４０】

電子透かし検出を行いコピーの可否を判断した結果、コピー可能であればＬＣＭによる楽曲の圧縮（ＡＴＲＡＣ３などによる帯域圧縮）及び暗号化を行ってから、携帯型機器２０へのコピーを行う（ステップＳ１１４→Ｓ１１１）。また、コピー不可であれば、ステップＳ１１５に進み、コピー処理を中止する。

【０１４１】

これまでに説明した実施形態ではいずれも、情報処理端末１０は、ＣＤから読み込んだ楽曲がコピー可能であることを確認できた後に、データ・コンテンツの圧縮暗号化及び携帯型機器２０へのコピー処理に移行するものである。これに対し、データ・コンテンツの圧縮暗号化処理の一部でコピー可否の確認処理を行う

こともできる。

【０１４２】

図９には、ＬＣＭでの帯域圧縮過程のデータをデータベースに対する照合データとして用いることができるコンテンツ・コピー管理システム１－２の構成例を示し、また、図１０には、該システム１－２において情報処理端末１０が実行する処理手順をフローチャートの形式で示している。

【０１４３】

データ圧縮プロセスは、一般に、ＤＣＴ（Discrete Cosine Transform：離散コサイン変換）、量子化、及びハフマン符号化で構成される。ＭＰ３（MPEG-1 Audio Layer-III）やＡＴＲＡＣなどの帯域圧縮ではｍＤＣＴ（変形離散コサイン変換）が用いられている。ｍＤＣＴは、直交変換の１つであり、時間軸領域を周波数領域に変換する。また、直交変換には、ｍＤＣＴ以外にも、ＤＣＴ（離散コサイン変換）、ｗａｖｅｌｅｔ（”ｗａｖｅｌｅｔ”は米サマス・テクノロジーズ社が開発した波形分析技術）などがある

【０１４４】

この実施形態に係るシステム１－２では、情報処理端末１０は、ＬＣＭプロセスにおいて生成されたｍＤＣＴ係数のハッシュ値を求めて、これをサーバ３０側に転送してデータベースと照合するようになっている。

【０１４５】

データベースと照合した結果、コピー可であれば、そのまま圧縮及び暗号処理を進めて、携帯型機器２０へのデータ・コピーを行う。他方、コピー不可と判断された場合には、Ｓｃｒｅｅｎｉｎｇ処理に戻って、電子透かし検出を行い、その検出結果に従ってコピーの可否を再度判断する。

【０１４６】

本実施形態によれば、情報処理端末１０は、Ｓｃｒｅｅｎｉｎｇ処理が完了していなくても、コピー用データの圧縮などの処理を並行して行うことができるので、コピー処理全体に要する時間が短縮化される。また、圧縮・暗号化されたコピー用データを作成しても、コピー不可と判断されたときには最終的に携帯型機器２０へのコピーを行わなければコンテンツ保護上も問題はない。また、ｍＤＣ

Ｔなどの圧縮過程でのデータは、通常、ＰＣＭ（Pulse Code Modulation）データよりもデータ量が少ないので、照合用データとしては都合がよい。

【０１４７】

以下、図１０に示すフローチャートを参照しながら、情報処理端末１０において実行される処理手順について説明する。

【０１４８】

まず、ＣＤ－ＲＯＭドライブ（図示しない）に装填されたＣＤから、ＩＳＲＣ（International Standard Recording Code）若しくはこれと同等のコンテンツ識別情報を取得する（ステップＳ１２１）。

【０１４９】

次いで、ＣＤから所望の楽曲データを読み込んで、端末１０内のハード・ディスク（図示しない）にコピーしておく（ステップＳ１２２）。

【０１５０】

次いで、ＬＣＤ処理の第１段階としてｍＤＣＴを実行して、楽曲データのｍＤＣＴ係数を計算する（ステップＳ１２３）。さらに、ｍＤＣＴ係数をハッシュ関数にかけてそのハッシュ値を計算する（ステップＳ１２４）。

【０１５１】

次いで、問合せ先となるサーバ３０と接続し（ステップＳ１２５）、さらにサーバ３０と認証及び鍵交換を行うことにより（ステップＳ１２６）、サーバ３０との安全な通信路を確保する。

【０１５２】

そして、情報処理端末１０は、ステップＳ１２１において読み込んだＩＳＲＣコードと、ステップＳ１２４において計算したハッシュ値とをサーバ３０側に転送して、ＣＤの調査を要求する（ステップＳ１２７）。

【０１５３】

ＣＤ調査要求に対して、サーバ３０側では、ＩＳＲＣコードを基に自身のデータベースを検索して、そのレコードが存在するか、さらにはそのハッシュ値が一致するか否かを判別して、その結果を情報処理端末１０側に返す（ステップＳ１２８）。

【０１５４】

情報処理端末１０側では、サーバ３０側からの返答を基に、楽曲データの携帯型機器２０へのコピーが許されるか否かを判別する。

【０１５５】

返答内容が、データベース中に該当するレコードが存在することを示していれば（ステップＳ１２９）、装填中のＣＤはデータベース登録されたものであり、電子透かしにより挿入されたデータは既知であるから、Ｓｃｒｅｅｎｉｎｇすなわち電子透かしの検出処理を省略することができる。この場合、ＣＤからのコピーの可否判断のみを行う（ステップＳ１３０、Ｓ１３１）。登録ＣＤは１回のみコピーが許容されているとすれば、ステップＳ１３０において、装填中のメディアがＣＤ－Ｒか否かをチェックすればよい。

【０１５６】

コピー可能であれば、量子化及びハフマン符号化という圧縮処理の残りの過程を実行する（ステップＳ１３２）。そして、圧縮データをさらに暗号化して携帯型機器２０へのコピーを行う（ステップＳ１３３）。これに対し、コピー不可であれば、ステップＳ１３４に進み、コピー処理を中止する。

【０１５７】

他方、ステップＳ１２９において、サーバ３０側のデータベースに該当レコードが存在しない、すなわち装填中のＣＤが登録ＣＤではないと判定された場合には、Ｓｃｒｅｅｎｉｎｇすなわち電子透かし検出処理を行う他ない（ステップＳ１３５）。

【０１５８】

電子透かし検出を行いコピーの可否を判断した結果、コピー可能であれば、量子化及びハフマン符号化という圧縮処理の残りの過程を実行する（ステップＳ１３２）。そして、圧縮データをさらに暗号化して携帯型機器２０へのコピーを行う（ステップＳ１３３）。また、コピー不可であれば、ステップＳ１３７に進み、コピー処理を中止する。

【０１５９】

上述したような情報処理端末１０における音楽データのコピー機能を、専用の

ハードウェア構成を備えた端末装置によって実現することも可能であるが、汎用的な処理が可能な一般的な計算機システム上で、図３、図５、図７、図１０の各フローチャートで示した処理手順をコンピュータ可読形式で記述したコンテンツ・コピー・アプリケーションを実行するという形態でも、本発明を実装することができる。

【０１６０】

図１１には、本発明に係る情報処理端末１０を実現することができる計算機システム１００のハードウェア構成を模式的に示している。以下、同図を参照しながら、システム１００内の各構成要素について説明する。

【０１６１】

システム１００のメイン・コントローラであるＣＰＵ（Central Processing Unit）１０１は、オペレーティング・システム（ＯＳ）の制御下で、各種のアプリケーションを実行する。ＣＰＵ１０１は、例えば、図３、図５、図７、図１０の各フローチャートで示した処理手順をコンピュータ可読形式で記述したコンテンツ・コピー・アプリケーションを実行することができる。図示の通り、ＣＰＵ１０１は、バス１０８によって他の機器類（後述）と相互接続されている。

【０１６２】

メモリ１０２は、ＣＰＵ１０１において実行されるプログラム・コードを格納したり、プログラム実行中の作業データを一時保管するために使用される記憶装置である。同図に示すメモリ１０２は、不揮発及び揮発メモリ双方を含むものと理解されたい。

【０１６３】

ディスプレイ・コントローラ１０３は、ＣＰＵ１０１が発行する描画命令を実際に処理するための専用コントローラである。ディスプレイ・コントローラ１０３において処理された描画データは、例えばフレーム・バッファ（図示しない）に一旦書き込まれた後、ディスプレイ１１１によって画面出力される。

【０１６４】

入力機器インターフェース１０４は、キーボード１１２やマウス１１３などのユーザ入力機器を計算機システム１００に接続するための装置である。

【０１６５】

ネットワーク･インターフェース１０５は、Ｅｔｈｅｒｎｅｔなどの所定の通信プロトコルに従って、システム１００をＬＡＮ（Local Area Network）などの局所的ネットワーク、さらにはインターネットのような広域ネットワークに接続することができる。

【０１６６】

ネットワーク上では、複数のホスト端末（図示しない）がトランスペアレントな状態で接続され、分散コンピューティング環境が構築されている。計算機システム１００とサーバ３０をネットワーク経由で接続することも可能であり、サーバ３０に対してデータベース問い合わせを行うことができる。また、ネットワーク上では、ソフトウェア・プログラムやデータ・コンテンツなどの配信が行うことができる。例えば、図３、図５、図７、図１０の各フローチャートで示した処理手順をコンピュータ可読形式で記述したコンテンツ･コピー･アプリケーションを、ネットワーク経由で計算機システム１００にダウンロードすることができる。また、コピー対象となる音楽データなどを、ネットワーク経由で配信することもできる。

【０１６７】

外部機器インターフェース１０７は、ハード･ディスク･ドライブ（ＨＤＤ）１１４やメディア･ドライブ１１５などの外部装置をシステム１００に接続するための装置である。

【０１６８】

ＨＤＤ１１４は、記憶担体としての磁気ディスクを固定的に搭載した外部記憶装置であり（周知）、記憶容量やデータ転送速度などの点で他の外部記憶装置よりも優れている。ソフトウェア・プログラムを実行可能な状態でＨＤＤ１１４上に置くことをプログラムのシステムへの「インストール」と呼ぶ。通常、ＨＤＤ１１４には、ＣＰＵ１０１が実行すべきオペレーティング･システムのプログラム･コードや、アプリケーション･プログラム、デバイス･ドライバなどが不揮発的に格納されている。

【０１６９】

例えば、図３、図５、図７、図１０の各フローチャートで示した処理手順をコンピュータ可読形式で記述したコンテンツ･コピー･アプリケーションを、ＨＤＤ１１４上にインストールすることができる。また、コピー対象となる音楽データなどを、ＨＤＤ１１４上に一時的に保存することもできる。ＣＤなどの記録メディアから読み出された音楽データは、例えばＷＡＶ形式のコンピュータ･ファイルとして、ＨＤＤ１１４上に保存される。

【０１７０】

メディア･ドライブ１１５は、ＣＤ（Compact Disc）やＭＯ（Magneto-Optical disc）、ＤＶＤ（Digital Versatile Disc）などの可搬型メディアを装填して、そのデータ記録面にアクセスするための装置である。

【０１７１】

可搬型メディアは、主として、ソフトウェア･プログラムやデータ･ファイルなどをコンピュータ可読形式のデータとしてバックアップすることや、これらをシステム間で移動（すなわち販売･流通･配布を含む）する目的で使用される。例えば、図３、図５、図７、図１０の各フローチャートで示した処理手順をコンピュータ可読形式で記述したコンテンツ･コピー･アプリケーションを、これら可搬型メディアを利用して複数の機器間で物理的に流通・配布することができる。また、コピー対象となる音楽データなどを、これら可搬型メディアを利用して機器間で物理的に流通・配布することができる。

【０１７２】

図１１に示すような計算機システム１００の一例は、米ＩＢＭ社のパーソナル･コンピュータ”ＰＣ／ＡＴ（Personal Computer/Advanced Technology）”の互換機又は後継機である。勿論、他のアーキテクチャを備えたコンピュータを、本実施形態に係る計算機システム１００として適用することも可能である。

【０１７３】

また、上述したようなサーバ３０による音楽データのコピー制御機能並びに電子透かし検出の代行機能を、専用のハードウェア構成を備えた端末装置によって実現することも可能であるが、汎用的な処理が可能な一般的な計算機システム上で、図４、図６、図８の各フローチャートで示した処理手順をコンピュータ可読

形式で記述したコンテンツ･コピー制御並びに電子透かし検出代行サーバ･アプリケーションを実行するという形態でも、本発明を実装することができる。

【０１７４】

図１２には、本発明に係るサーバ３０を実現することができる計算機システム２００のハードウェア構成を模式的に示している。以下、同図を参照しながら、システム２００内の各構成要素について説明する。

【０１７５】

システム２００のメイン・コントローラであるＣＰＵ（Central Processing Unit）２０１は、オペレーティング･システム（ＯＳ）の制御下で、各種のアプリケーションを実行する。ＣＰＵ２０１は、例えば、図４、図６、図８の各フローチャートで示した処理手順をコンピュータ可読形式で記述したコンテンツ･コピー制御並びに電子透かし検出代行サーバ･アプリケーションを実行することができる。図示の通り、ＣＰＵ２０１は、バス２０８によって他の機器類（後述）と相互接続されている。

【０１７６】

メモリ２０２は、ＣＰＵ２０１において実行されるプログラム･コードを格納したり、プログラム実行中の作業データを一時保管するために使用される記憶装置である。同図に示すメモリ２０２は、不揮発及び揮発メモリ双方を含むものと理解されたい。

【０１７７】

ディスプレイ・コントローラ２０３は、ＣＰＵ２０１が発行する描画命令を実際に処理するための専用コントローラである。ディスプレイ･コントローラ１０３において処理された描画データは、例えばフレーム・バッファ（図示しない）に一旦書き込まれた後、ディスプレイ２１１によって画面出力される。

【０１７８】

入力機器インターフェース２０４は、キーボード２１２やマウス２１３などのユーザ入力機器を計算機システム２００に接続するための装置である。

【０１７９】

ネットワーク･インターフェース２０５は、Ｅｔｈｅｒｎｅｔなどの所定の通

信プロトコルに従って、システム２００をＬＡＮ（Local Area Network）などの局所的ネットワーク、さらにはインターネットのような広域ネットワークに接続することができる。

【０１８０】

ネットワーク上では、複数のホスト端末（図示しない）がトランスペアレントな状態で接続され、分散コンピューティング環境が構築されている。計算機システム２００と情報処理端末１０をネットワーク経由で接続することも可能であり、情報処理端末１０からデータベース問い合わせを受けることができる。また、ネットワーク上では、ソフトウェア・プログラムやデータ・コンテンツなどの配信が行うことができる。例えば、図４、図６、図８の各フローチャートで示した処理手順をコンピュータ可読形式で記述したコンテンツ･コピー制御並びに電子透かし検出代行サーバ･アプリケーションを、ネットワーク経由で計算機システム２００にダウンロードすることができる。また、コピー対象となる音楽データなどを、ネットワーク経由で配信することもできる。

【０１８１】

データベース・インターフェース２０７は、ハード･ディスク･ドライブ（ＨＤＤ）２１４のようなデータベースを構築するための外部装置をシステム１００に接続するための装置である。データベース２１４上では、各楽曲に関する電子透かし情報やコピー可否情報などがデータベース管理されており、情報処理端末１０からのＩＳＲＣなどの楽曲の識別情報や属性情報に基づく問い合わせに応じることができる（前述）。

【０１８２】

また、ＨＤＤ２１４は、記憶担体としての磁気ディスクを固定的に搭載した外部記憶装置であり（周知）、記憶容量やデータ転送速度などの点で他の外部記憶装置よりも優れている。ソフトウェア・プログラムを実行可能な状態でＨＤＤ２１４上に置くことをプログラムのシステムへの「インストール」と呼ぶ。通常、ＨＤＤ２１４には、ＣＰＵ２０１が実行すべきオペレーティング･システムのプログラム･コードや、アプリケーション･プログラム、デバイス･ドライバなどが不揮発的に格納されている。例えば、図４、図６、図８の各フローチャートで示

した処理手順をコンピュータ可読形式で記述したコンテンツ･コピー制御並びに電子透かし検出代行サーバ･アプリケーションを、ＨＤＤ２１４上にインストールすることができる。

【０１８３】

図１２に示すような計算機システム２００の一例は、米ＩＢＭ社のパーソナル･コンピュータ”ＰＣ／ＡＴ（Personal Computer/Advanced Technology）”の互換機又は後継機である。勿論、他のアーキテクチャを備えたコンピュータを、本実施形態に係る計算機システム２００として適用することも可能である。

【０１８４】

［追補］

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。

【０１８５】

本明細書中では、ＣＤに記録された音楽データのコピーを行う場合を例にとって本発明の実施形態を説明したが、本発明の適用範囲はこれに限定されるものではない。例えば映像や静止画など他のデータ・コンテンツに対しても、あるいはＤＶＤやＭＤなど他の記録メディアから読み取ったデータに対しても、本発明は同様に作用効果を奏することができる。

【０１８６】

要するに、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０１８７】

【発明の効果】

以上詳記したように、本発明によれば、コンテンツに埋め込まれた電子透かしを検査することができる、優れた電子透かし検査技術を提供することができる。

【０１８８】

また、本発明によれば、コンテンツに埋め込まれた電子透かしを検査した結果

に従ってコンテンツの複製の可否を判断することができる、優れた電子透かし検査技術を提供することができる。

【０１８９】

また、本発明によれば、計算負荷の高い電子透かし検査処理を代行して、コンテンツの複製の可否を判断することができる、優れた電子透かし検査技術を提供することができる。

【０１９０】

本発明では、コンテンツの複製を行う計算機システム自体がスクリーニングすなわち電子透かしの検出を必ずしも行わず、別の手段により、コンテンツのコピー制御情報を取得できるようにした。例えば、コンテンツには電子透かしが挿入されていないことがあらかじめ分かっているＣＤからコピーするような場合には、かかるＣＤであることを確認できれば、電子透かしの検出処理そのものをスキップして、コピー所要時間を短縮化する。

【０１９１】

すなわち、本発明によれば、データから電子透かしを検出する必要がないので処理時間が短縮化され、ユーザの利便性が向上する。

【０１９２】

また、電子透かしを検出する場合であっても、コンテンツ（例えば楽曲）全体にわたって検出する必要がないので、処理時間が短縮化され、ユーザの利便性が向上する。

【図面の簡単な説明】

【図１】

ＳＤＭＩで想定しているＳｃｒｅｅｎｉｎｇ処理を実現するための機能ブロック図である。

【図２】

本発明の実施例に係るコンテンツ・コピー管理システム１の全体構成を模式的に示した図である。

【図３】

本発明の第１の実施形態に係るコンテンツ・コピー管理システム１において、

情報処理端末１０上でＣＤ上の音楽データを携帯型機器２０にコピーするときの、情報処理端末１０側で実行する処理手順を示したフローチャートである。

【図４】

本発明の第１の実施形態に係るコンテンツ・コピー管理システム１において、情報処理端末１０上でＣＤ上の音楽データを携帯型機器２０にコピーするときの、サーバ３０側で実行する処理手順を示したフローチャートである。

【図５】

本発明の第１の実施形態に係るコンテンツ・コピー管理システム１において、情報処理端末１０上でＣＤ上の音楽データを携帯型機器２０にコピーするときの、情報処理端末１０側で実行する処理手順の他の例を示したフローチャートである。

【図６】

本発明の第１の実施形態に係るコンテンツ・コピー管理システム１において、情報処理端末１０上でＣＤ上の音楽データを携帯型機器２０にコピーするときの、サーバ３０側で実行する処理手順の他の例を示したフローチャートである。

【図７】

サーバ３０側のデータベースに対して問合せを行うことによって電子透かし検出処理を省略するための、情報処理端末１０上で実行する処理手順のさらに他の例を示したフローチャートである。

【図８】

サーバ３０側のデータベースに対して問合せを行うことによって電子透かし検出処理を省略するための、情報処理端末１０上で実行する処理手順のさらに他の例を示したフローチャートである。

【図９】

ＬＣＭでの帯域圧縮過程のデータをデータベースに対する照合データとして用いることができるコンテンツ・コピー管理システム１－２の構成を模式的に示した図である。

【図１０】

コンテンツ・コピー管理システム１－２において情報処理端末１０が実行する

処理手順を示したフローチャートである。

【図１１】

情報処理端末１０として適用可能な計算機システム１００の構成を模式的に示した図である。

【図１２】

サーバ３０として適用可能な計算機システム２００の構成を模式的に示した図である。

【符号の説明】

１…コンテンツ・コピー管理システム

１０…情報処理端末

２０…携帯型機器

３０…サーバ

１００…計算機システム（情報処理端末）

１０１…ＣＰＵ，１０２…メモリ

１０３…ディスプレイ・コントローラ

１０４…入力機器インターフェース

１０５…ネットワーク・インターフェース

１０７…外部機器インターフェース，１０８…バス

１１１…ディスプレイ，１１２…キーボード，１１３…マウス

１１４…ハード・ディスク装置，１１５…メディア・ドライブ

２００…計算機システム（サーバ）

２０１…ＣＰＵ，２０２…メモリ

２０３…ディスプレイ・コントローラ

２０４…入力機器インターフェース

２０５…ネットワーク・インターフェース

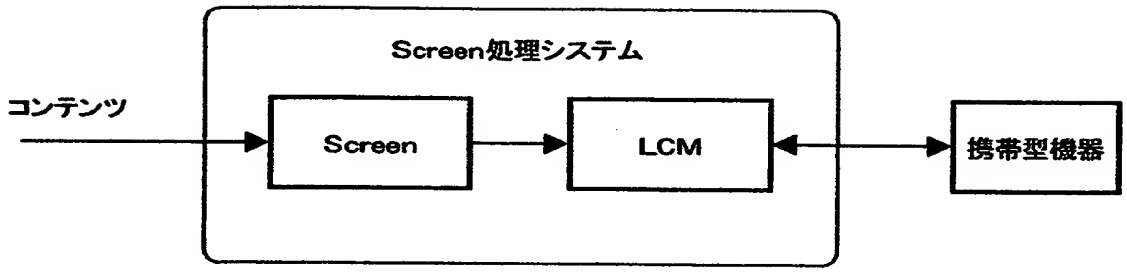
２０７…データ･ベースインターフェース，２０８…バス

２１１…ディスプレイ，２１２…キーボード，２１３…マウス

２１４…データベース

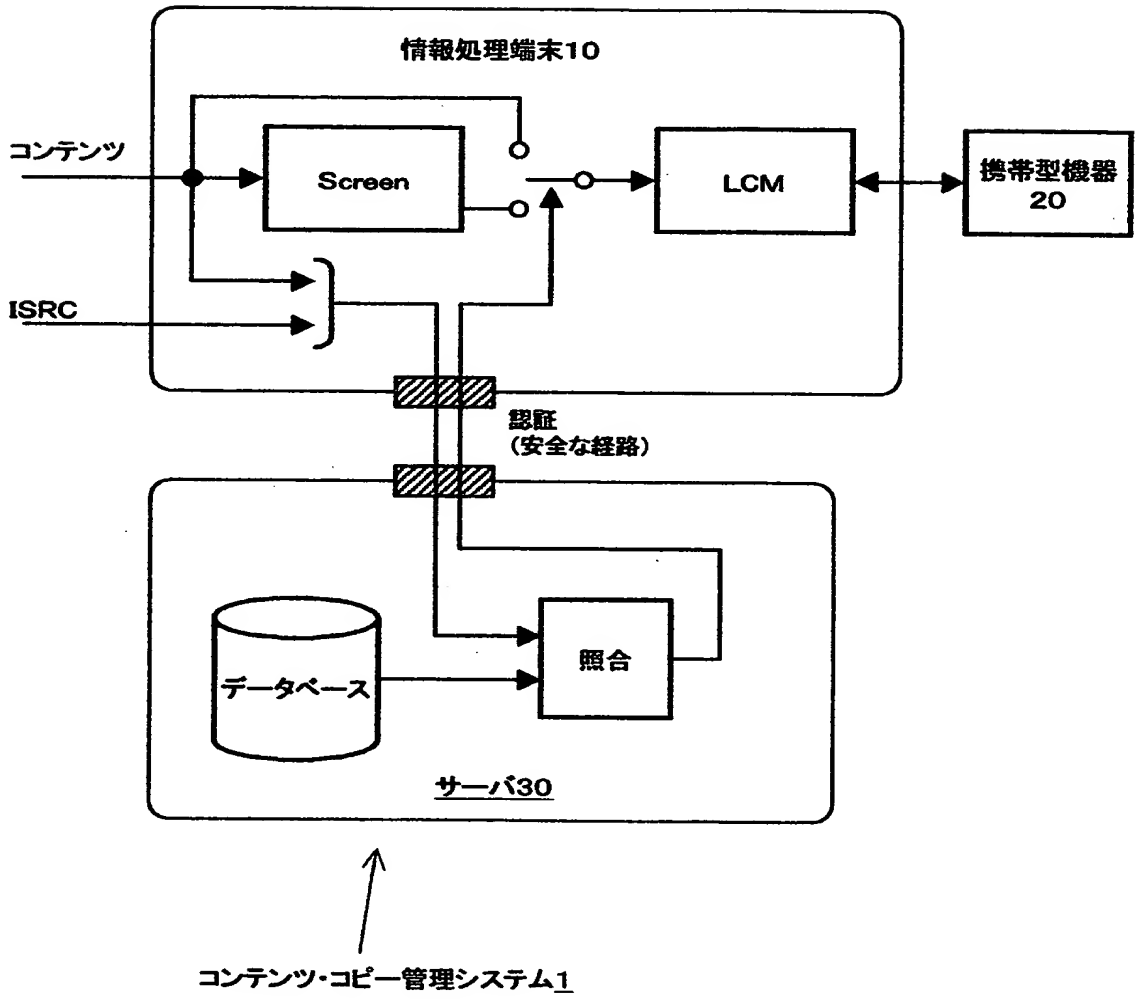
【書類名】　　図面

【図１】



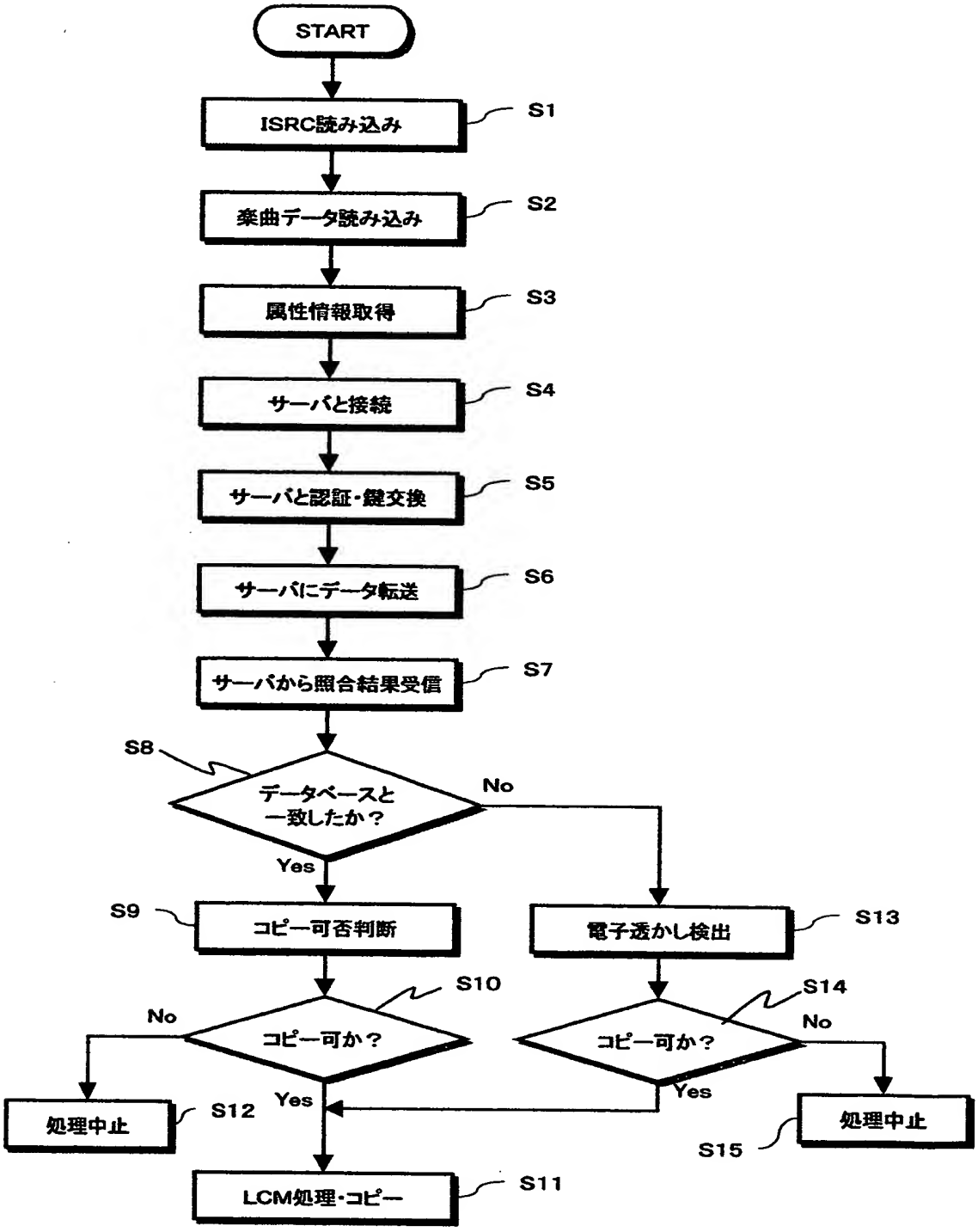
出証特２００１－３０３９９０２

【図２】

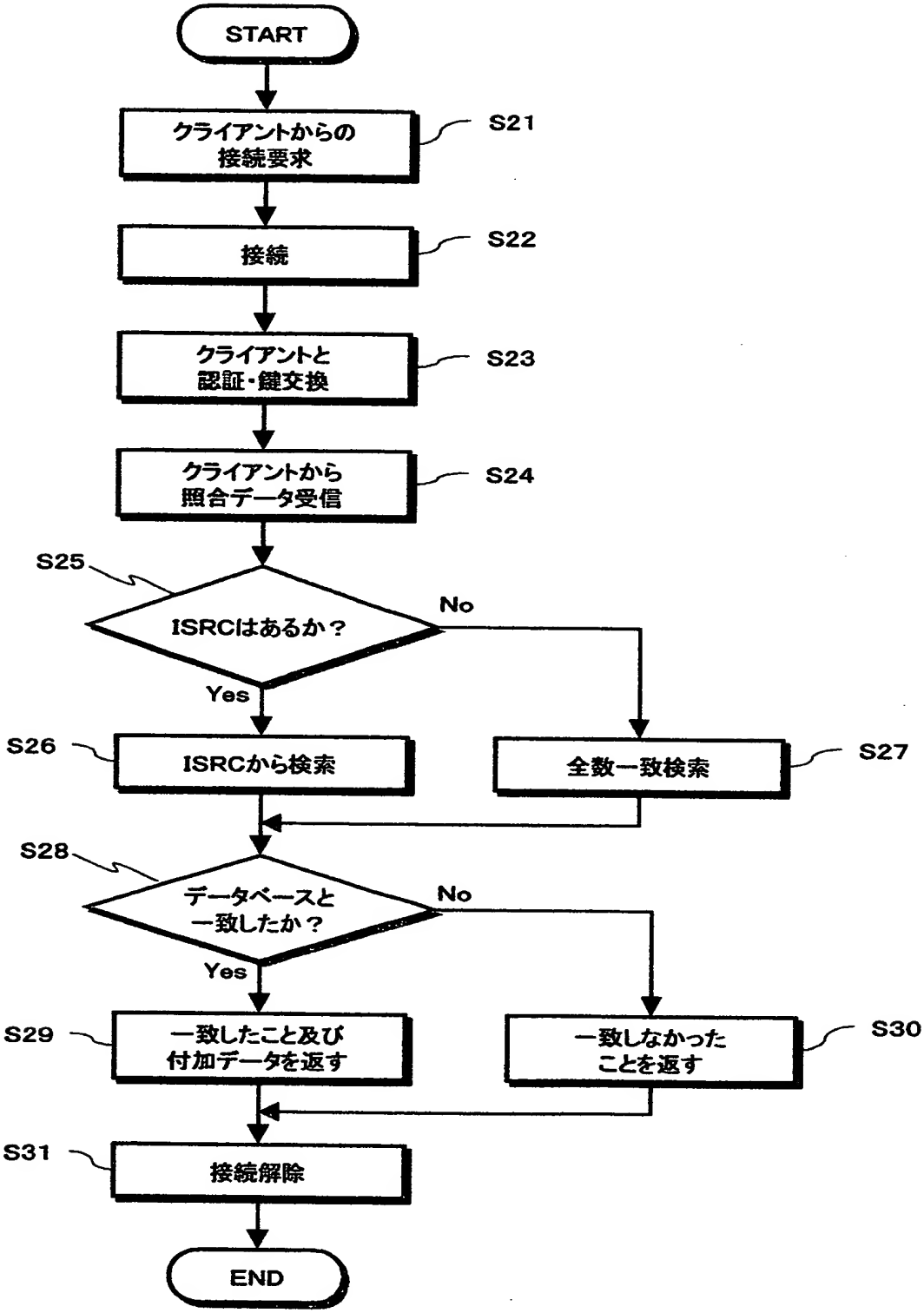


出証特２００１－３０３９９０２

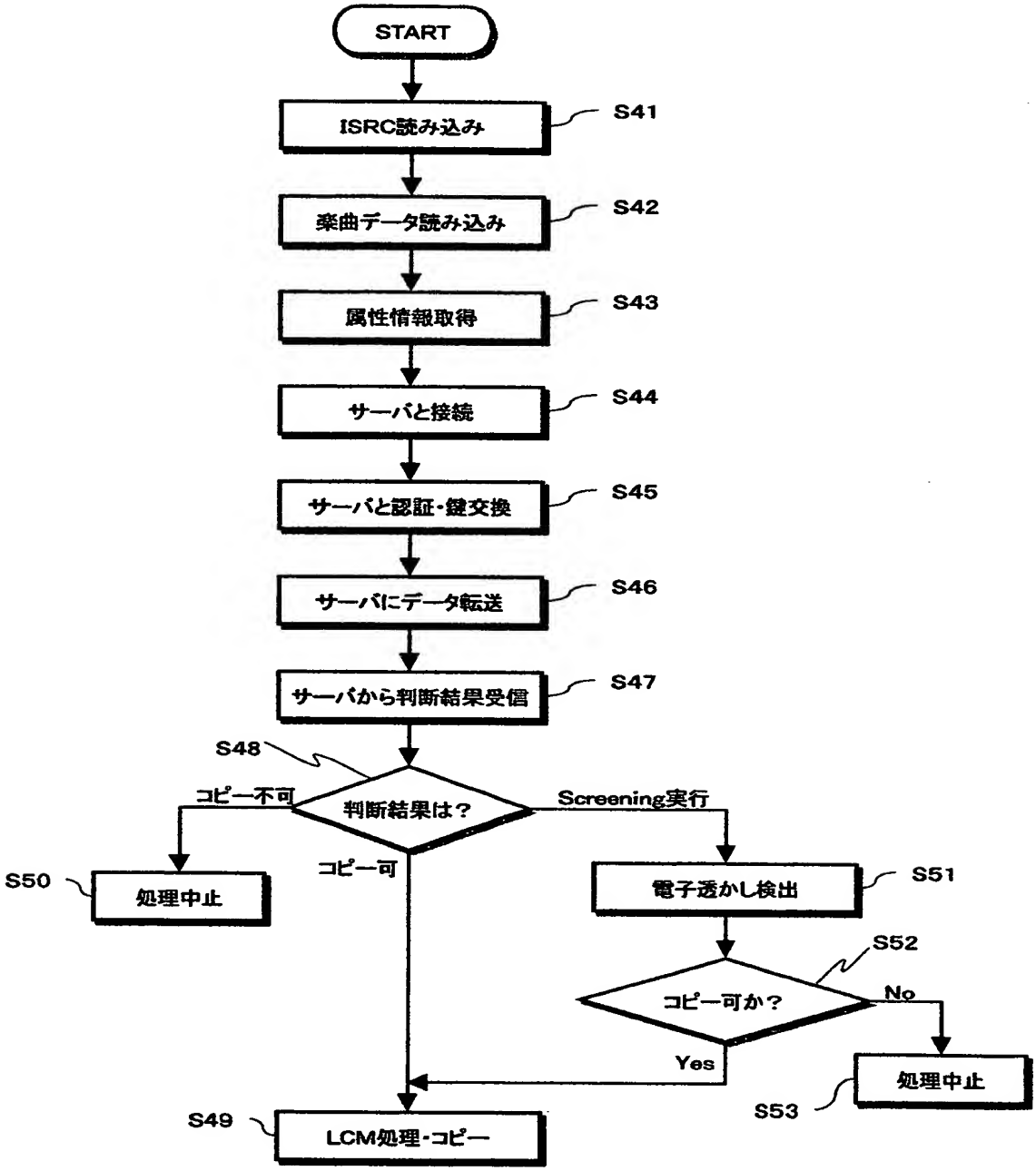
【図３】


START
ISRC読み込み
S1
楽曲データ読み込み
S2
属性情報取得
S3
サーバと接続
S4
サーバと認証・鍵交換
S5
サーバにデータ転送
S6
サーバから照合結果受信
S7
S8
データベースと一致したか？
No
Yes
S9
コピー可否判断
S10
No
コピー可か？
処理中止
S12
Yes
LCM処理・コピー
S11
電子透かし検出
S13
S14
コピー可か？
No
Yes
処理中止
S15

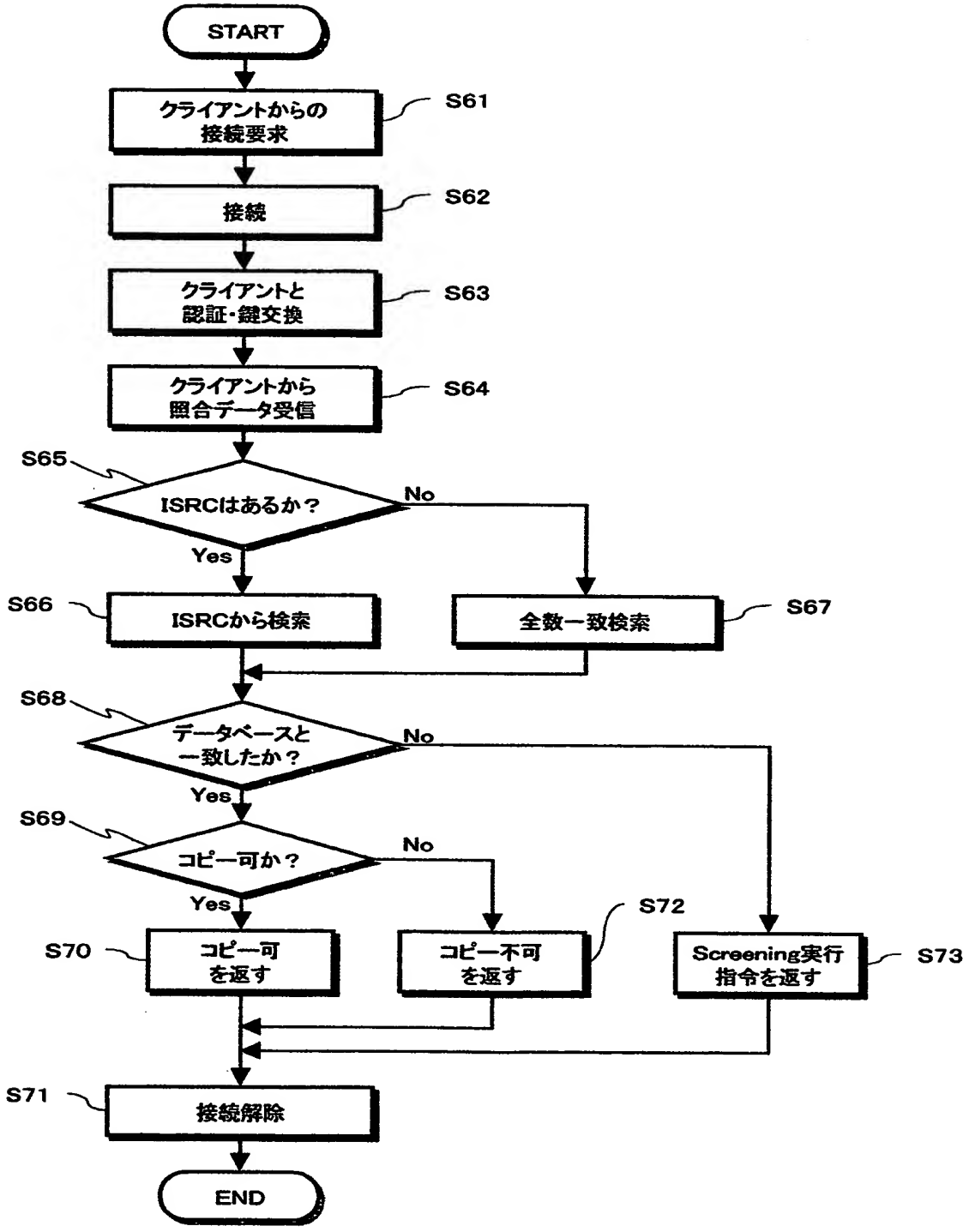
【図４】


START
クライアントからの接続要求
S21
接続
S22
クライアントと認証・鍵交換
S23
クライアントから照合データ受信
S24
S25
ISRCはあるか？
No
Yes
S26
ISRCから検索
全数一致検索
S27
S28
データベースと一致したか？
No
Yes
S29
一致したこと及び付加データを返す
一致しなかったことを返す
S30
S31
接続解除
END

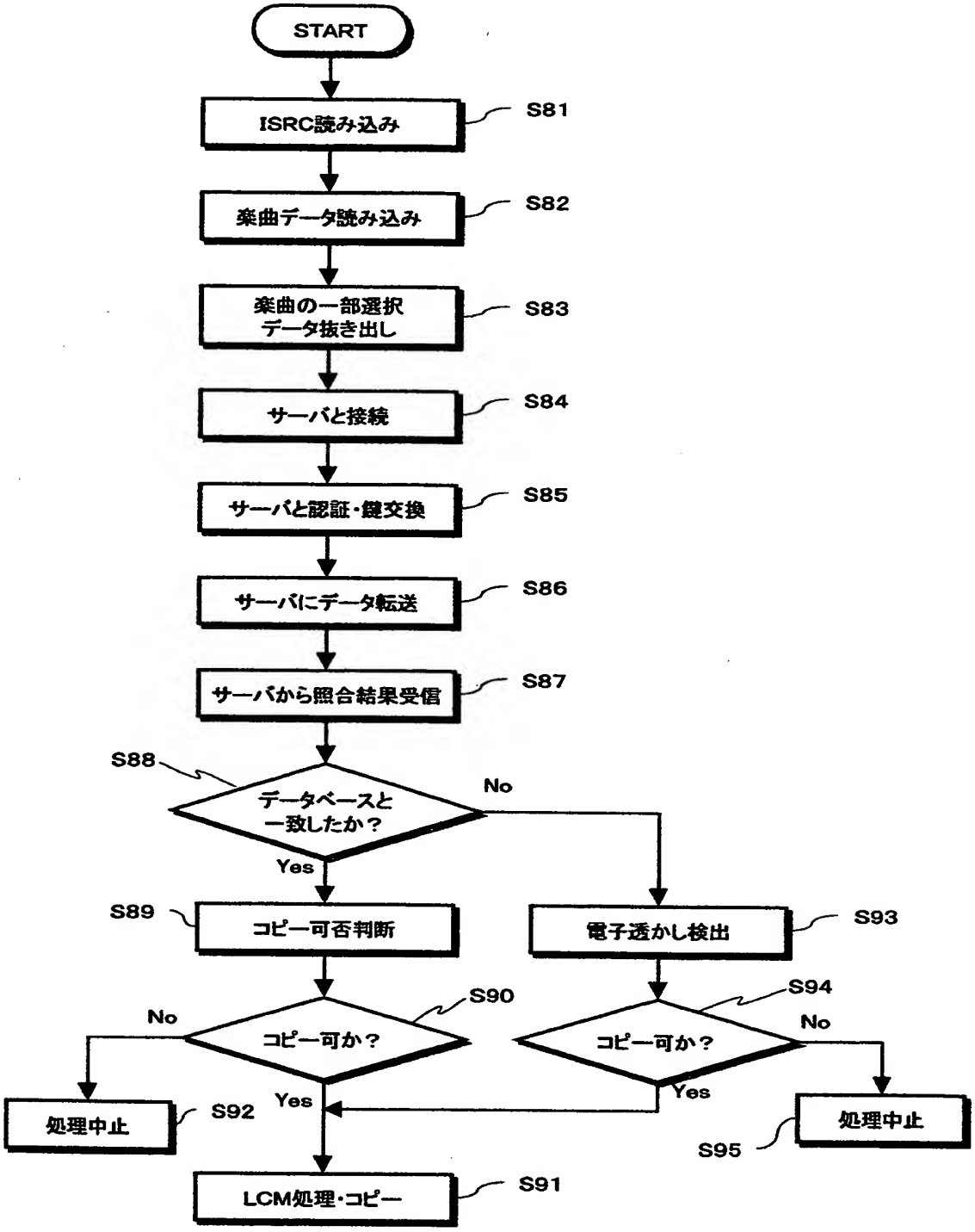
【図５】


START
ISRC読み込み
S41
楽曲データ読み込み
S42
属性情報取得
S43
サーバと接続
S44
サーバと認証・鍵交換
S45
サーバにデータ転送
S46
サーバから判断結果受信
S47
S48
判断結果は？
コピー不可
Screening実行
コピー可
S50
処理中止
電子透かし検出
S51
S52
コピー可か？
No
Yes
処理中止
S53
S49
LCM処理・コピー

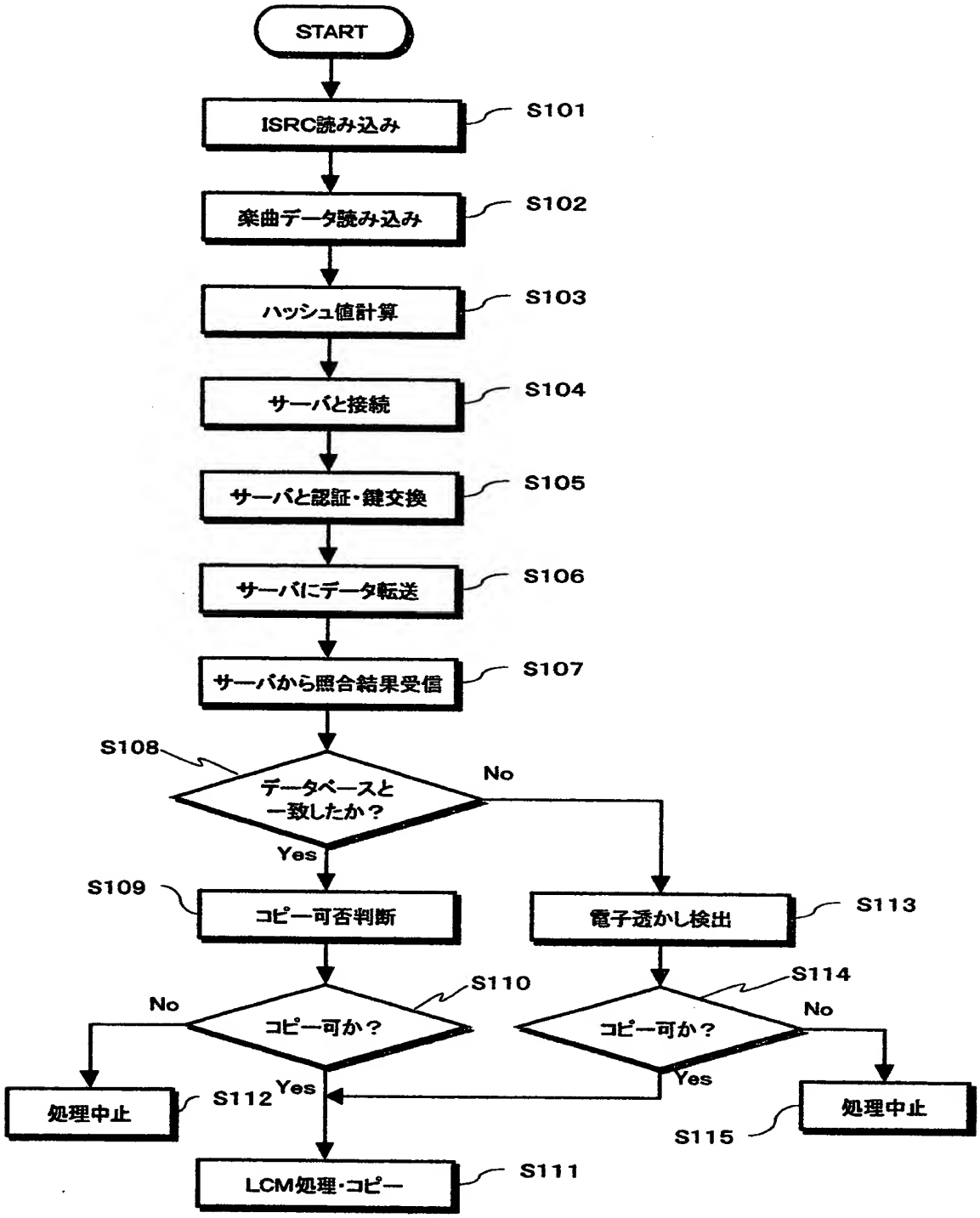
【図６】


START
クライアントからの接続要求
S61
接続
S62
クライアントと認証・鍵交換
S63
クライアントから照合データ受信
S64
S65
ISRCはあるか？
No
Yes
S66
ISRCから検索
全数一致検索
S67
S68
データベースと一致したか？
No
Yes
S69
コピー可か？
No
Yes
S70
コピー可を返す
コピー不可を返す
S72
Screening実行指令を返す
S73
S71
接続解除
END

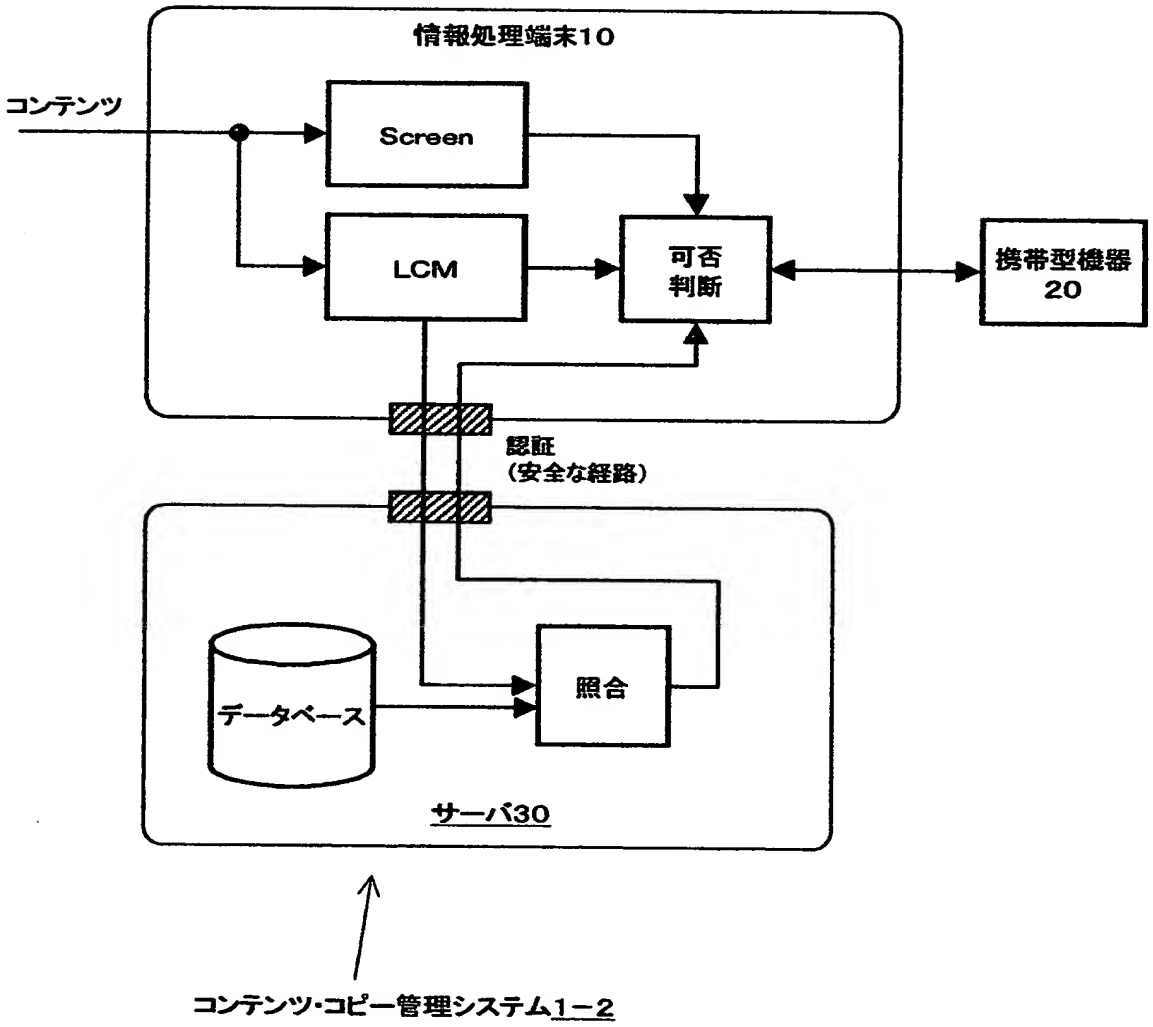
【図７】


START
ISRC読み込み
S81
楽曲データ読み込み
S82
楽曲の一部選択
データ抜き出し
S83
サーバと接続
S84
サーバと認証・鍵交換
S85
サーバにデータ転送
S86
サーバから照合結果受信
S87
S88
データベースと
一致したか？
No
Yes
S89
コピー可否判断
電子透かし検出
S93
S90
コピー可か？
No
S94
コピー可か？
No
Yes
Yes
処理中止
S92
処理中止
S95
LCM処理・コピー
S91

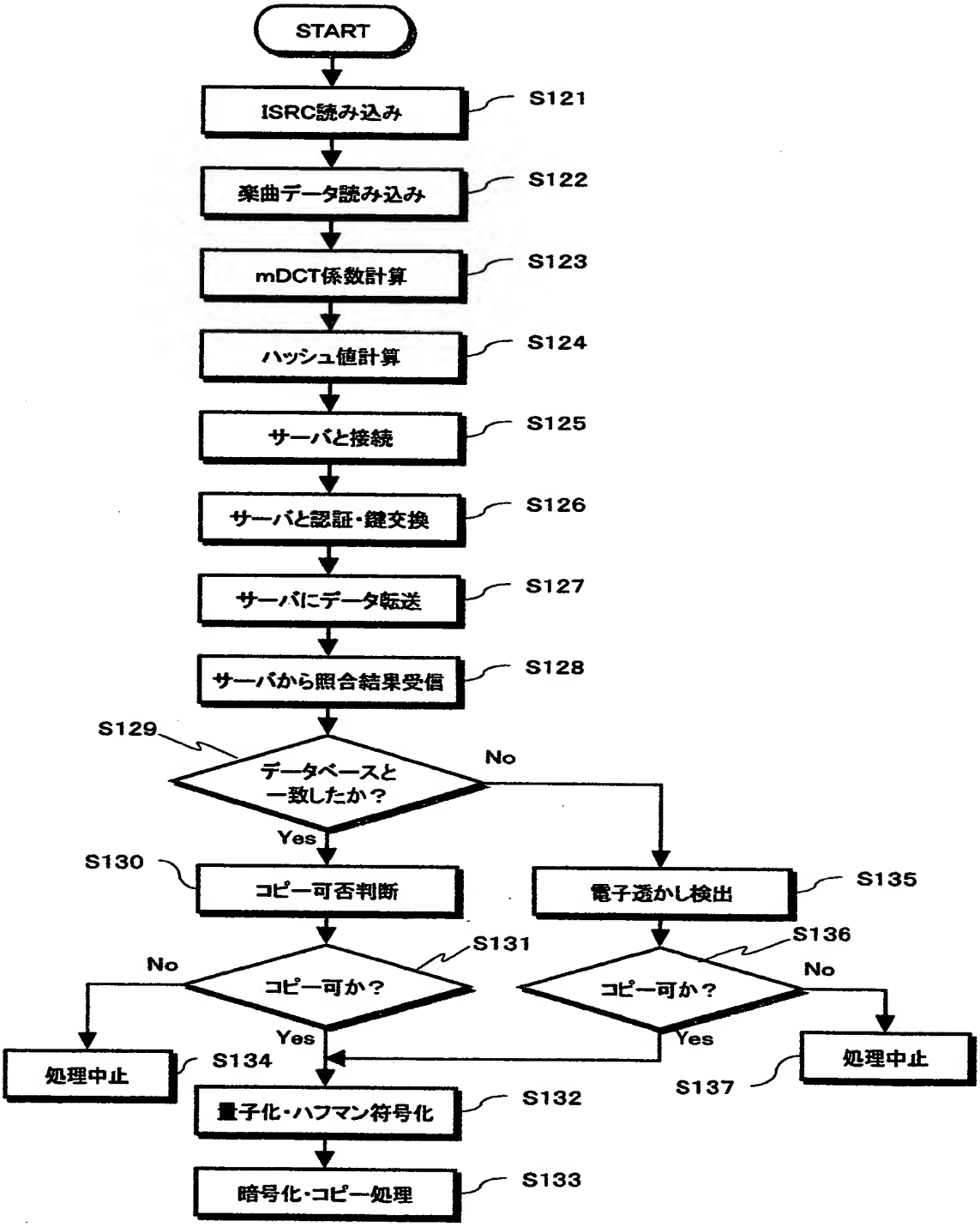
【図８】


START
ISRC読み込み
S101
楽曲データ読み込み
S102
ハッシュ値計算
S103
サーバと接続
S104
サーバと認証・鍵交換
S105
サーバにデータ転送
S106
サーバから照合結果受信
S107
S108
データベースと一致したか？
No
Yes
S109
コピー可否判断
S110
No
コピー可か？
Yes
処理中止
S112
LCM処理・コピー
S111
S113
電子透かし検出
S114
コピー可か？
No
Yes
処理中止
S115

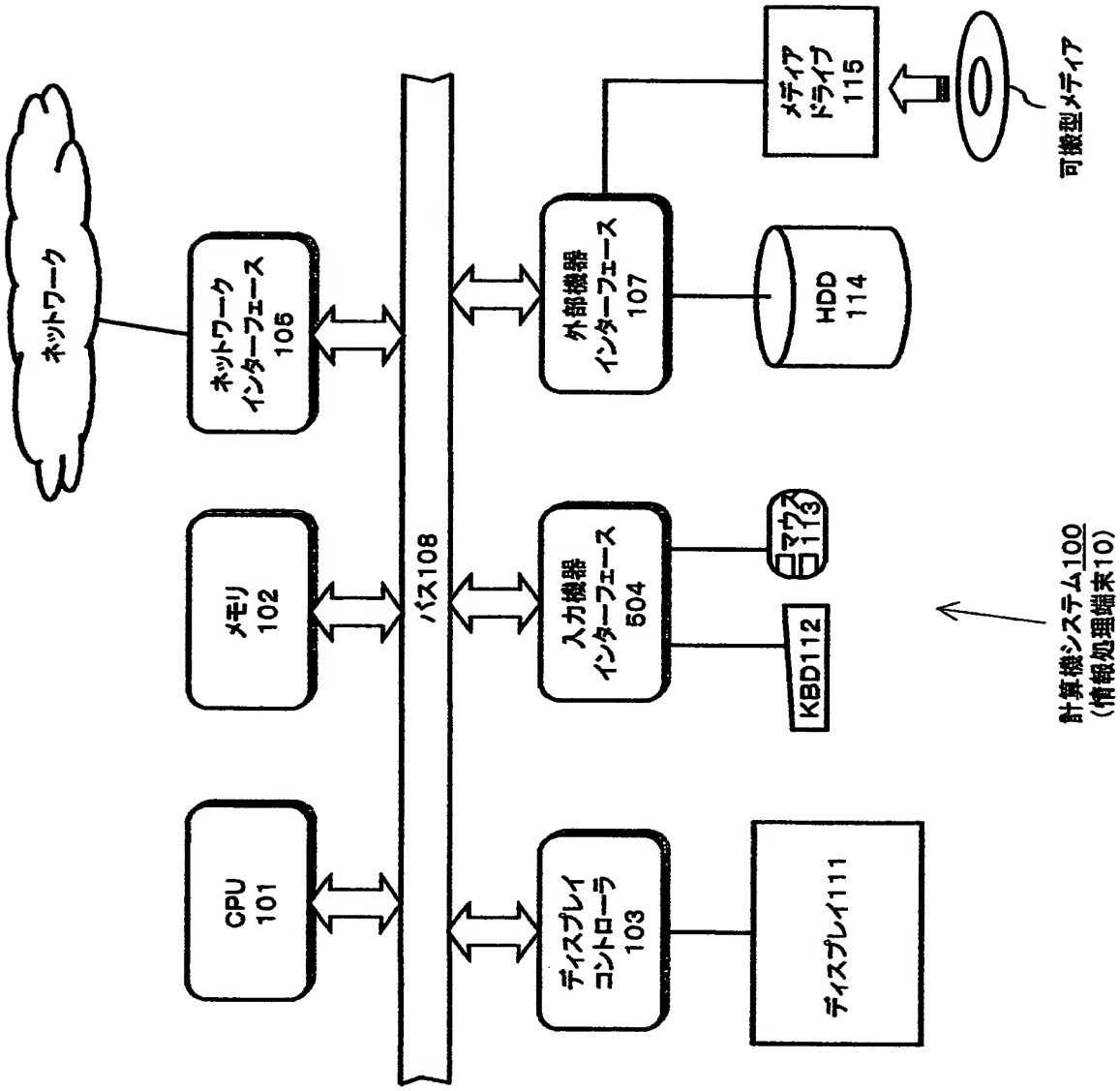
【図９】


情報処理端末10
コンテンツ
Screen
LCM
可否
判断
携帯型機器
20
認証
(安全な経路)
データベース
照合
サーバ30
コンテンツ・コピー管理システム1－2

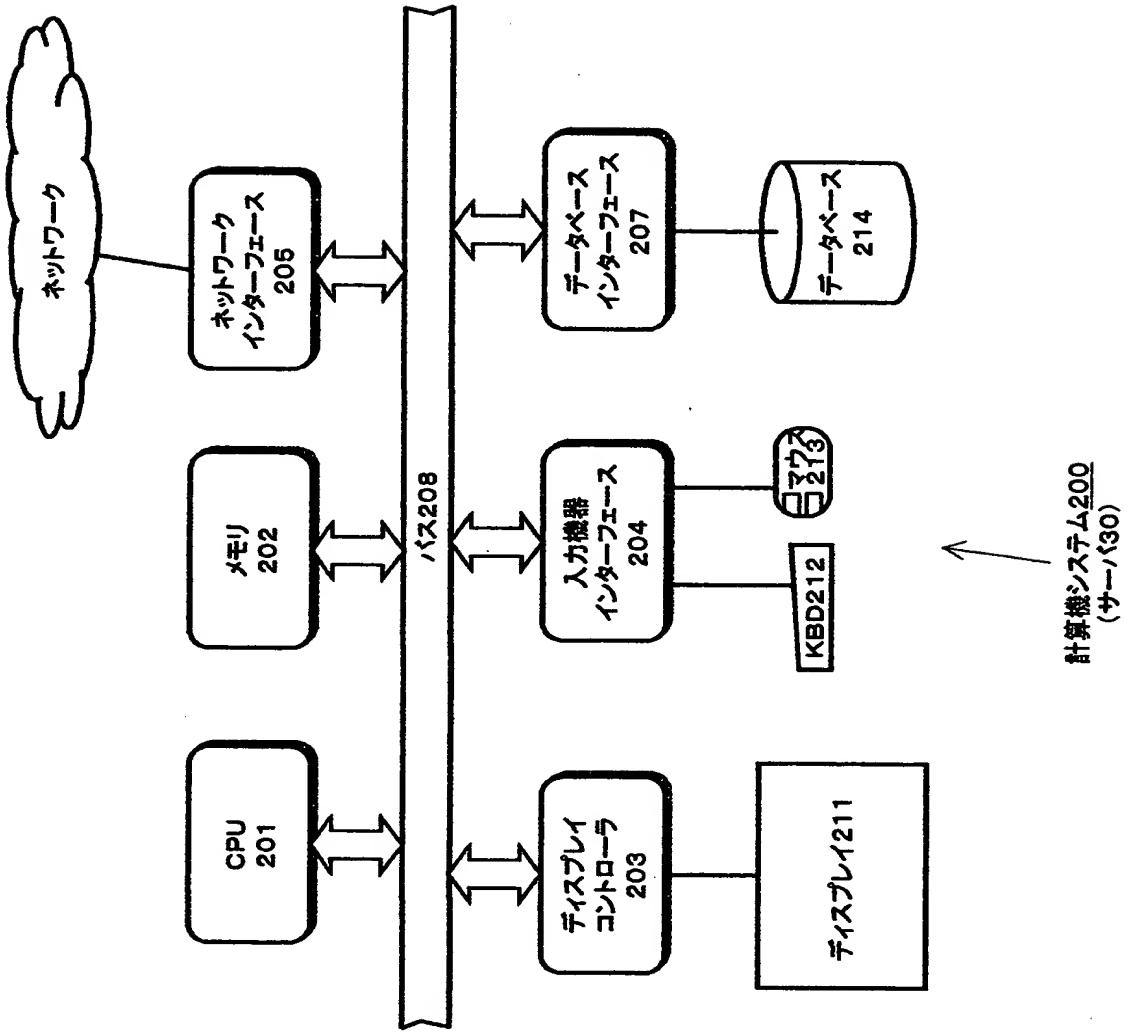
【図１０】


START
ISRC読み込み
S121
楽曲データ読み込み
S122
mDCT係数計算
S123
ハッシュ値計算
S124
サーバと接続
S125
サーバと認証・鍵交換
S126
サーバにデータ転送
S127
サーバから照合結果受信
S128
S129
データベースと一致したか？
No
Yes
S130
コピー可否判断
S131
No
コピー可か？
Yes
処理中止
S134
S135
電子透かし検出
S136
コピー可か？
No
Yes
処理中止
S137
量子化・ハフマン符号化
S132
暗号化・コピー処理
S133

【図１１】


ネットワーク
ネットワーク
インターフェース
106
メモリ
102
CPU
101
バス108
外部機器
インターフェース
107
入力機器
インターフェース
504
ディスプレイ
コントローラ
103
メディア
ドライブ
115
HDD
114
KBD112
ディスプレイ111
可搬型メディア
計算機システム100
(情報処理端末10)

【図１２】


ネットワーク
ネットワーク
インターフェース
205
メモリ
202
CPU
201
バス208
データベース
インターフェース
207
入力機器
インターフェース
204
ディスプレイ
コントローラ
203
データベース
214
マウス
213
KBD212
ディスプレイ211
計算機システム200
(サーバ30)

【書類名】　　要約書

【要約】

【課題】　計算負荷の高い電子透かし検査処理を代行して、コンテンツの複製の可否を判断する。

【解決手段】　コンテンツの複製を行う計算機システム自体がスクリーニングすなわち電子透かしの検出を必ずしも行わず、外部サーバのような別の手段により、コンテンツのコピー制御情報を取得できるようにした。例えば、コンテンツには電子透かしが挿入されていないことがあらかじめ分かっているＣＤからコピーするような場合には、かかるＣＤであることを確認できれば、電子透かしの検出処理そのものをスキップして、コピー所要時間を短縮化する。

【選択図】　図２

認定・付加情報

特許出願の番号	特願２００１－１０３１５３
受付番号	５０１００４８２３７４
書類名	特許願
担当官	第三担当上席　　００９２
作成日	平成１３年　４月　５日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】　000002185

【住所又は居所】　東京都品川区北品川６丁目７番３５号

【氏名又は名称】　ソニー株式会社

【代理人】　申請人

【識別番号】　100101801

【住所又は居所】　東京都中央区新富１－１－７　銀座ティーケイビル６階　澤田・宮田・山田特許事務所

【氏名又は名称】　山田　英治

【選任した代理人】

【識別番号】　100093241

【住所又は居所】　東京都中央区新富１－１－７　銀座ティーケイビル６階　澤田・宮田・山田特許事務所

【氏名又は名称】　宮田　正昭

【選任した代理人】

【識別番号】　100086531

【住所又は居所】　東京都中央区新富１－１－７　銀座ティーケイビル６階澤田・宮田・山田特許事務所

【氏名又は名称】　澤田　俊夫

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社